2014-12-01

Classifying and Cataloging Cyber-Security Incidents Within Cyber-Physical Systems

William B. Miller
Brigham Young University - Provo

Classifying and Cataloging Cyber-Security Incidents

Within Cyber-Physical Systems

William B. Miller

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
Joseph J. Ekstrom
C. Richard G. Helps

School of Technology

Brigham Young University

December 2014

ABSTRACT

Classifying and Cataloging Cyber-Security Incidents Within Cyber-Physical Systems

William B. Miller
School of Technology, BYU
Master of Science

In the past, there were perceived delineations between the cyber world and the physical world. We are becoming increasingly aware of the overlap between these two worlds, and the overlap itself is increasing. The overlap between these two worlds is known as cyber-physical systems.

There have been several incidents involving cyber-physical systems and the number of these incidents is increasing dramatically. In the past there has been no effort to identify methods for describing these incidents in the unique context of cyber-physical systems.

This research provides a taxonomy for classifying these incidents that focuses on cross domain, impact oriented analysis. A repository for information about these incidents has also been created as part of this research.

Keywords: William Miller, cyber-physical systems, cyber-security, incident, taxonomy, database

ACKNOWLEDGEMENTS

First and foremost, I would like to acknowledge the support of my family. My wife, Erica, and my children, Eleanor, Matthew, Jarom, and Margaret, have been supportive and patient with me as I have gone through this process. I am sincerely grateful for their support.

I would also like to thank Dr. Rowe and Dr. Helps for their participation in the CPS research group that provided the foundation and feedback for most of this work. Another thank you to my boss, Hans Douma, for his encouragement in pursuing my schooling and his willingness to make my studies possible while maintaining employment. Finally, I would like to thank Ross Woodside for his work on the development of the database and web front-end for this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

In today's world, there is an increasing overlap between the cyber world and the physical world. We are seeing increasing numbers of "things" that are being controlled by computers. These "things" are also being connected to each other in ways that have never been seen before. These types of "things" include large scale industrial control systems that manage our critical infrastructure such as power plants, manufacturing, and transportation systems. They also include vehicles, medical devices, home automation systems, and smartphones and other mobile devices. Figure 1-1 illustrates how cyber systems and physical systems overlap in cyber-physical systems. This overlap is increasing as we continue to look for new ways to control the physical world (Rajkumar et al. 2010).

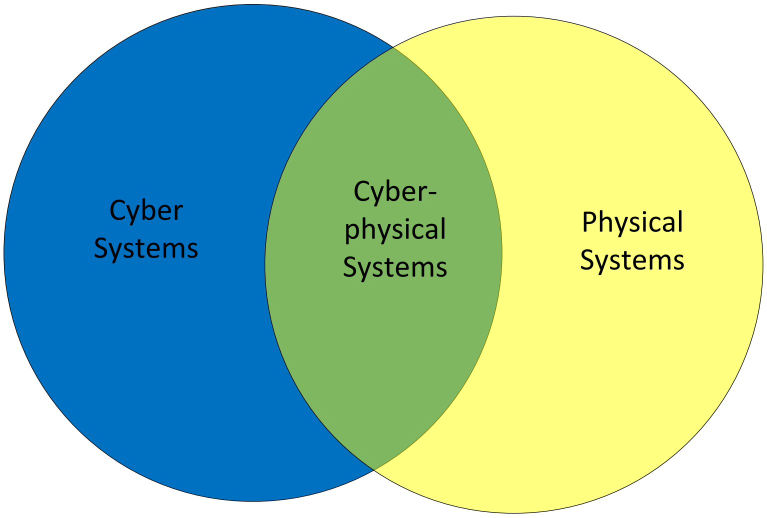


Figure 1-1: Cyber-Physical Systems

These cyber-physical systems present security challenges that are similar in many ways to purely cyber systems, but there are also some areas where the challenges are unique to cyber-physical systems.

1.1 Problem

In 2012, an attempt was made to identify some of the security incidents within critical infrastructure systems (Miller and Rowe 2012). In making this attempt it was discovered that the problems presented in securing our critical infrastructure are more pronounced than was initially understood. Three key issues were identified as this analysis was attempted. First, the issues related to attacks on critical infrastructure are present in the broader realm of all Cyber-Physical Systems (CPS). Figure 1-2 demonstrates how critical infrastructure is a subset of CPS as a whole. Second, the taxonomies currently in use do not sufficiently describe incidents within the realm of CPS due to their focus on purely cyber systems. Finally, it was discovered that there is not a current public source of information about these incidents.

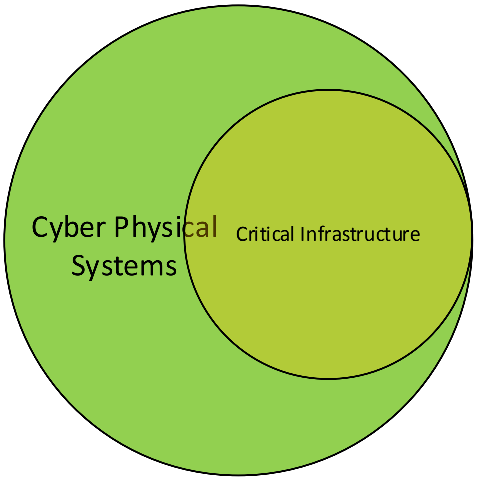


Figure 1-2: Critical Infrastructure as a sub-set of Cyber-Physical Systems

One of the heightened risks with cyber-attacks against critical infrastructure is the physical component to these attacks. An attack in this area is not limited to information or processes. The physical components of these systems suggest that any impact on the information also has a possibility of causing an impact within the physical world. While the impact on physical systems is obvious and well publicized for ICS and SCADA systems, it is not limited to these types of systems. There are many other systems that have a presence in the cyber world and the physical world at the same time. While many incidents within critical infrastructure may be on a large scale, an incident on a smaller CPS is no less impactful to those involved. For example, an incident in a medical CPS could be fatal for those involved. All types of CPSs should be included in these efforts to protect the infrastructure.

There are several incident taxonomies currently available to classify cyber-security incidents. There are some that focus on the nature of an attack, while others describe the defensive posture of the victim. There are also some that attempt to detail the impact of the attack. All of these taxonomies contain weaknesses when attempting to apply them to incidents involving a CPS. For example, the taxonomy developed by Howard and Longstaff describes how an attack was carried out along with the informational target of an attack and resultant effects. This taxonomy does not consider the entity where the attack occurred (Howard and Longstaff 1998). The AVOIDIT taxonomy is another example of a taxonomy that is focused on how an attack was carried out with no consideration for the entity where the attack occurred (Simmons et al. 2009). Blackwell's taxonomy describes the defensive posture of the victim of an attack also without describing the entity that was the victim (Blackwell 2010). The taxonomy presented by Kjaerland describes the entity where the attack occurred and the informational effects of the attack

(Kjaerland 2006). None of these taxonomies account for the physical effects of an attack. They also do not account for incidents that may not be a targeted attack.

The taxonomies that are focused on the nature of an attack are adequate if the goal is to understand how an attack was carried out, but these taxonomies do not account for the impact of an attack on the target or other victims that may not be directly targeted. Further, focusing on the means of an attack does not account for incidents that do not stem from a malicious attack, but still cause an impact to people and to the system.

A taxonomy that focuses on the defensive posture of the victim is helpful in understanding what weaknesses were present in the defenses of a victim, but these taxonomies are also inadequate in describing the impact of an incident, or dealing with incidents that do not involve a malicious attack.

Taxonomies that attempt to detail the impact of an attack also suffer from many weaknesses, especially in dealing with CPS incidents. These taxonomies are typically focused on the impact to information in an attack. They do not contemplate the physical impacts that occur within CPS incidents. These taxonomies are also focused on an attack and do not consider incidents that do not fall under the category of an attack yet have an impact on people, property or the system.

The ability to classify incidents within a CPS is only one part of the problem. A repository of information about the incidents that have occurred that is available for academic research would facilitate the ability to study these incidents and devise methods to prevent future incidents.

There are industry incident databases that detail all incidents whether there is a cyber-component or not. These databases are designed for members of the industry and are not available for academic research without incurring significant costs (RISI 2014). There are also cyber-security incident databases, but these do not address the physical components of an incident within a CPS (US-CERT 2014). A method of cataloging incidents within a CPS that is freely available for academic research would enhance the ability to protect these systems in the future.

A cross domain, impact oriented classification system and database are needed to facilitate better research into the nature and impact of these types of incidents. This would allow researchers to be able to identify the similarities in incidents as well as understand the impacts across multiple sectors of cyber-physical systems.

1.2 Research Questions

This research attempted to answer the following questions:

- Q1. What taxonomy categories will allow for cross domain analysis of incidents?
- Q2. What taxonomy categories will allow for an impact oriented analysis of incidents?
- H1. Suitable methods for measuring the impact of an incident currently exist.
- H2. Currently available methods can be adapted for use in CPS incidents.
- Q3. What are the identifiable benefits of a cross domain classification system?
- Q4. What are the identifiable benefits of an impact oriented classification system?

1.2.1 Taxonomy Categories

There are differing ideas on how to classify cyber-security incidents in general. These differences also extend to incidents within a CPS. Some classification systems focus on the method of attack, others focus on the defensive posture of the victim. There are classification systems that attempt to be general purpose systems that can be used in any type of incident, while others are more narrowly defined and only apply to specific use cases. For example, there are classification systems that describe specific methods of attack, or that are only applicable to a specific industry (US-CERT 2014; RISI 2014; OWASP).

With so many classification systems already available, some may question the need for a new system. All of these classification systems are applicable in the realm in which they were intended to be used, but when it comes to studying incidents within a CPS, we need a classification that allows for cross domain analysis. This system should be able to describe incidents within utility systems, health care systems, transportation systems, and any other domains that may involve a CPS.

The domain in which a CPS operates is not the only unique characteristic when studying incidents within a CPS. Incidents within a CPS have real world impacts. These impacts must be quantified in order to form a complete analysis of this type of an incident. This research will also identify the taxonomy categories that will allow for this type of impact oriented analysis.

1.2.2 Suitable Methods for Measuring the Impact of an Incident

There are currently methods for measuring the impact of purely physical incidents. These methods are generally associated with the security industry. This research will attempt to use these existing methods to describe the impact of a CPS incident.

1.2.3 Identifiable Benefits

This research attempts to create a method for cross domain, impact oriented analysis of incidents within a CPS. As part of this research, an attempt is made to identify the benefits of this type of analysis in contrast to existing approaches. The research attempts to identify what benefits may be achieved by this type of research that are not available in already existing methods of analyzing incidents.

1.3 Definitions

The following terms will be useful to understand when reading this thesis:

Critical Infrastructure – The systems that support and sustain society. Including utilities, transportation, and communications.

Cyber Component – The computing component of a CPS.

Cyber-physical System (CPS) – A system where technology intersects with the physical world.

Cyber-security Incident – An event in a system that causes an unauthorized impact to the system. This could be a targeted attack, an incidental attack, or an accident.

Hacktivist – An individual or group that utilizes unauthorized computer access and disruptive actions to achieve political or social goals.

Impact – The effect of a Cyber-security Incident. Both direct and indirect impacts are considered.

Industrial Control System (ICS) – A type of CPS designed to control industrial processes.

Market Sector – The industry or area in which a CPS is used.

Means – How a cyber-security incident occurred. This may describe the methods used by an attacker or the circumstances that lead to an accident.

Source Type – A description of the entity were a Cyber-security Incident originated.

Supervisory Control and Data Acquisition (SCADA) – An implementation of ICS that is used in much of the critical infrastructure.

Taxonomy – An ordered classification system.

Victim Type – A description of the entity where a cyber-security incident occurred.

1.4 Delimitations

This research has been limited by the following constraints. This research has classified and cataloged cyber-security incidents involving cyber-physical systems. This research has not attempted a classification of broader cyber-security incidents. This research has also been limited to incidents that involve both cyber and physical components. An attempt has not been made to classify or catalog incidents that contain only a cyber-component or only a physical component. For example, an incident that strictly focuses on stealing corporate secrets would not be included in this research. At the same time, an incident that strictly involved the failure of physical components has also not been included.

2 LITERATURE REVIEW

2.1 Introduction

A review of literature on cyber-physical systems is undertaken to document the current understanding of what constitutes a CPS and the unique challenges that are faced when identifying incidents in this area. There is also a discussion of currently available incident taxonomies to understand their uses and applicability to a CPS. This review includes examples of incidents within a CPS. Finally, a review of incident databases is undertaken in order to understand their availability and applicability to a CPS.

2.2 Cyber-Physical Systems

In modern society, we are seeing the increasing intersection of two formerly separate worlds. The intersection of the cyber world with the physical world is growing at a rapid pace (Poovendran 2010). These areas of intersection are known as a cyber-physical system (CPS) (Rajkumar et al. 2010). These systems provide a new set of challenges when it comes to preventing and responding to incidents. In the past, a cyber-security incident focused on the information that was involved in the incident. Now, we must also account for the physical impact that may occur from an incident. This impact may include property damage, disruption of services, or even serious injury or death.

2.2.1 Cyber-Physical Systems Characteristics

There is no clear-cut definition of what a CPS is. Rather, a CPS is more easily defined by its characteristics (Helps and Mensah 2012). The major characteristic of a CPS is its physical aspect. This physical aspect includes components such as sensors and actuators that are controlled by some form of computer system. This may be a large scale system such as Supervisory Control and Data Acquisition (SCADA) or a small system such as a smart phone or tablet.

In 2010, Radha Poovendran attempted to explain the CPS space. Poovendran discussed the emerging trends in the physical world, cyber-physical systems of today and tomorrow, complex interface and interactions between cyber and physical worlds, grand challenges and solutions in CPS, and the future of CPS community effort (Poovendran 2010).

Poovendran explains some of the emerging trends in the physical world. One of these trends is the increase in human mobility. During the 20th century, advances in transportation increased the distances humans could travel and decreased the time it would take to travel those distances. These advances even included placing a man on the moon (Poovendran 2010). Many of these advances in how we interact with the physical world were due to developments in cyber-physical systems. At that time, and continuing today, humans experience difficulties in their interactions with the physical world. For example, despite great advances in automotive technology, many still are injured or killed in accidents each year (Poovendran 2010).

There are many advancements taking place in the area of CPSs. Improvements in both the cyber and physical sectors are rapidly converging to create highly collaborative systems that are able to react to and control elements within the physical world. Poovendran argues that existing systems are capable of much greater interactions between the cyber and physical worlds.

Poovendran anticipates that in the future CPSs will become more integrally involved in several sectors of the economy (Poovendran 2010).

Poovendran also comments on the complexities of interaction between the cyber and physical worlds. The nature of the world is complex, parallel, continuous, and dynamically changing with many things happening at the same time. In the cyber world, there are discrete states and asynchronous interactions. These differences make the interactions between the cyber and physical worlds more complex. This interaction is particularly alarming due to the fact that human lives are affected by CPSs (Poovendran 2010).

There are many advances that need to be made in order to realize the true potential of CPSs. Poovendran notes there needs to be a dramatic increase in the ability to design for cyber and physical interactions at the same time. A CPS must also be able to quickly adapt to the constantly changing environment of the physical world. There also need to be changes to the education of engineers, computer programmers, and information technology professionals to manage the increasing complexity of CPSs. This educational change will require cross-disciplinary studies to provide the necessary understanding of all aspects of CPSs (Poovendran 2010).

Ragunathan Rajkumar and others also wrote about the characteristics of a CPS in 2010. They discussed the grand challenges and vision of CPSs, scientific foundations and challenges, and the social impact and infrastructure of CPSs. They also discussed the need for non-technical people to be able to interact with a CPS (Rajkumar et al. 2010).

Rajkumar et al. present several examples of what they term as the grand challenges and vision of CPSs. The first example is an advanced electric power grid. One of the current challenges of the power grid is that a failure in one part of the system may have a cascading effect that influences other parts of the system. This was evident in the 2003 Midwest blackout in the United States. Another challenge of the current power grid is the rapidly increasing introduction of renewable energy sources. Some of these sources, such as wind power, do not produce a regular power stream as is expected with traditional power sources. These challenges lead to the vision of an advanced power grid based on CPS technologies that is more robust and resilient to failures (Rajkumar et al. 2010). Figure 2-1 represents the advanced power grid envisioned by Rajkumar et al.

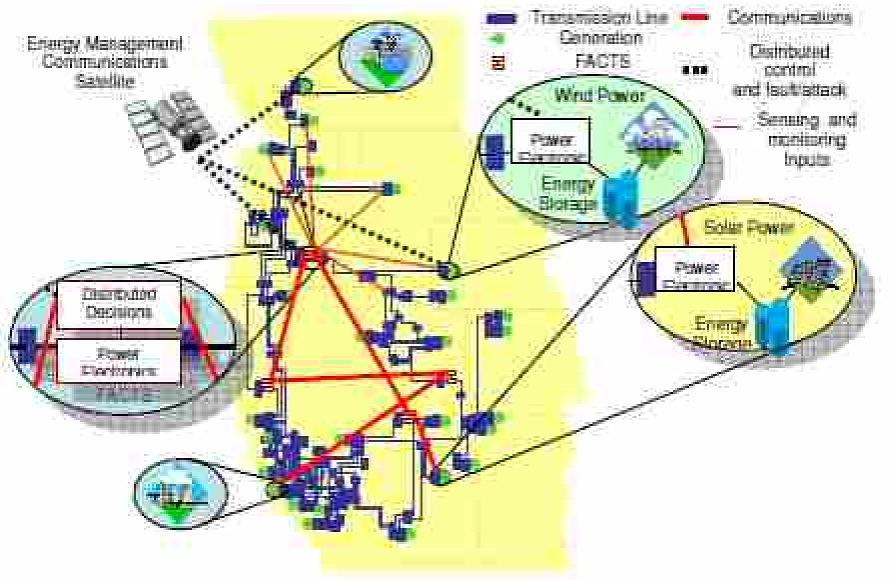


Figure 2-1: Vision of Advanced Power Grid

Another vision for CPSs that is presented is to aid the protection of our natural environment. Rajkumar et al. propose a vast network of sensors and actuators that is capable of providing fine-grained real-time data about environmental conditions. This network would drastically change the way scientific data is gathered and analyzed (Rajkumar et al. 2010).

The next area discussed is in disaster response or large-scale evacuations. The authors envision a large-scale managed transportation system that combines road, air, and rail traffic. This system could be used to coordinate large scale evacuations and more effectively utilize available resources (Rajkumar et al. 2010).

The final vision discussed concerns assistive devices. The authors envision devices that could aid the elderly or disabled with many of their daily tasks. These devices would be mostly autonomous, but would allow for voice commands or remote commands from a health care professional or family member. These types of devices would require levels of trust that do not currently exist with devices and communication channels (Rajkumar et al. 2010).

One of the issues with CPSs is the interconnected nature of these systems. Many CPSs were designed to be isolated systems. This is especially true of industrial control and SCADA systems. With the advent of the internet, many of these formerly isolated systems have been connected in ways that were never imagined by their designers. Many SCADA systems now have web based monitoring and control systems. These systems are even capable of being controlled by a mobile phone (Ozdemir and Karacor 2006).

2.3 Incident Taxonomies

There are many methods of classifying cyber-security incidents. Some have proposed general taxonomies that can be used for any incident. Others have proposed more specific taxonomies that deal with a particular type of incident or a specific type of target.

2.3.1 General Taxonomies

There have been many attempts to define a system for classifying cyber-attacks or incidents. These began as attempts to identify software vulnerabilities that could be compromised to form an attack. In 1998, Howard and Longstaff presented the first attempt at a unified security taxonomy. This taxonomy attempted to define an attack based on the tool used, the vulnerability exploited, the action taken, the target, and the unauthorized result (Howard and Longstaff 1998). Figure 2-2 presents Howard and Longstaff's incident taxonomy.

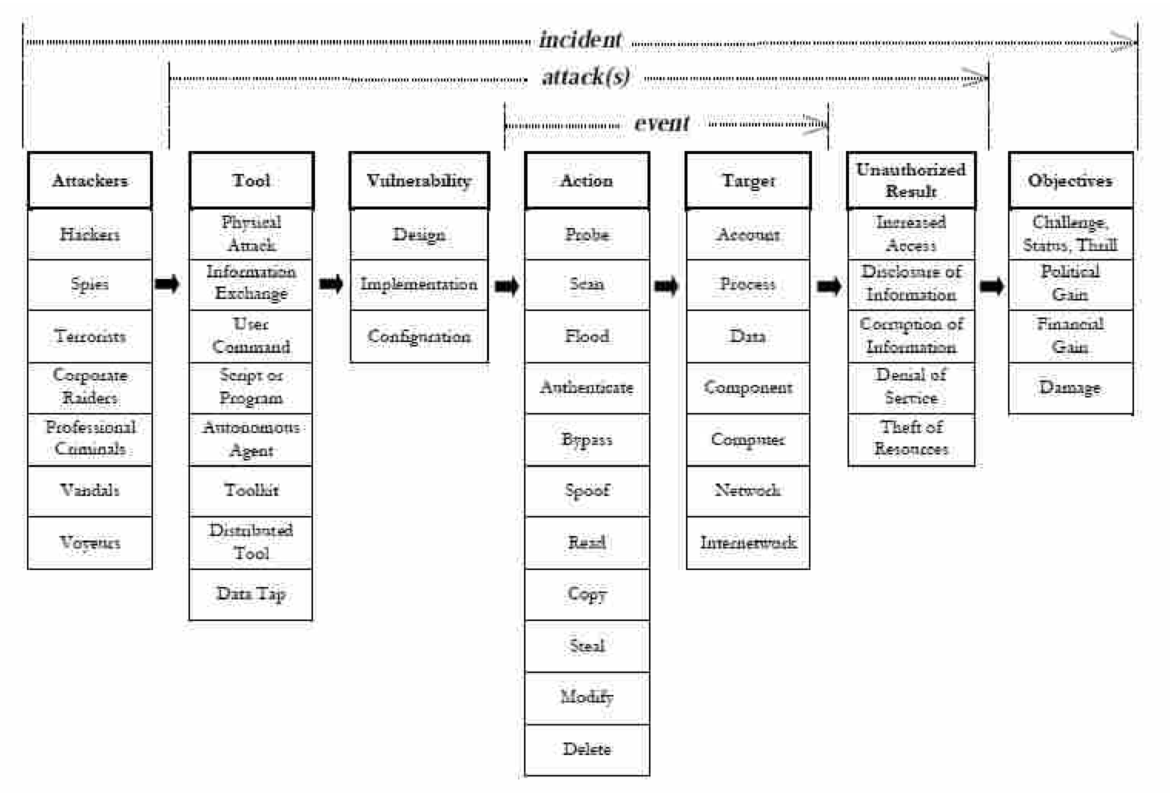


Figure 2-2: Howard and Longstaff's Incident Taxonomy

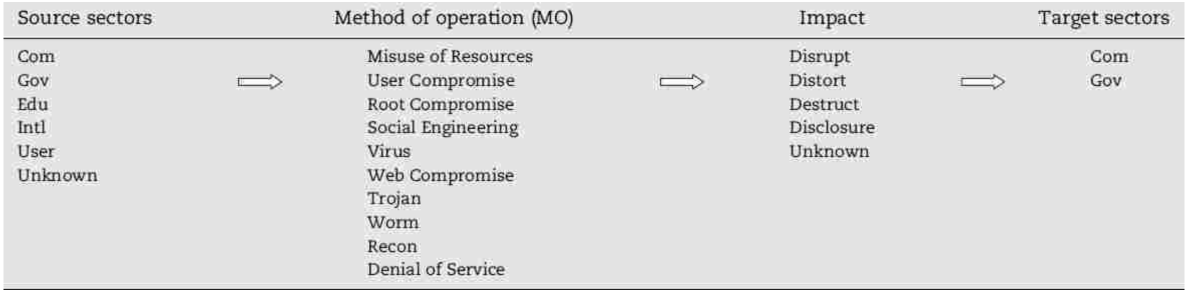
Howard and Longstaff begin their taxonomy by defining an event. An event comprises an action and a target. An event does not necessarily denote anything malicious or unwanted. There are thousands of legitimate events each day such as a user logging in to their account. There are other events that may be unwanted that still do not signify an attack.

An attack as defined by Howard and Longstaff is "a series of steps taken by an attacker to achieve an unauthorized result" (Howard and Longstaff 1998). This "series of steps" is broken down into the tool the attacker uses, the vulnerability that is exploited, the action that is performed on a target (event), and the unauthorized result that is desired. In essence, "An attacker uses a tool to exploit a vulnerability to perform an action on a target in order to achieve an unauthorized result" (Howard and Longstaff 1998).

An attack may be part of a group of attacks that can be classed together for some reason. These groups of attacks are termed incidents. Howard and Longstaff define an incident as "a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing" (Howard and Longstaff 1998).

There have been other attempts at defining incident taxonomies. Most of these have been extensions of the taxonomy created by Howard and Longstaff. In 2006, Maria Kjaerland proposed a taxonomy that included the source and target sectors along with the method of operations and the impact to the target (Kjaerland 2006).

Kjaerland describes an attack in terms of Source Sectors, MO, Impact, and Target Sectors. Source Sectors is the source of an incident and is meant to describe the attacker. MO is the method of operation in how the attack was carried out. Impact describes the results of the attack and how the target was affected. Target Sectors describe the victim of the attack (Kjaerland 2006). Figure 2-3 presents Kjaerland's incident taxonomy.



Source sectors		Method of operation (MO)		Impact		Target sectors
Com		Misuse of Resources		Disrupt		Com
Gov	⇨	User Compromise	⇨	Distort	⇨	Gov
Edu		Root Compromise		Destruct		
Intl		Social Engineering		Disclosure		
User		Virus		Unknown		
Unknown		Web Compromise				
		Trojan				
		Worm				
		Recon				
		Denial of Service				

Figure 2-3: Kjaerland's Incident Taxonomy

Kjaerland described the Source Sectors as Com, Gov, Edu, Intl, User, and Unknown. The MO or method of operation contained Misuse of Resources, User Compromise, Root

Compromise, Social Engineering, Virus, Web Compromise, Trojan, Worm, Recon, and Denial of Service. The options for Impact include Disrupt, Distort, Destruct, Disclosure, and Unknown. The Target Sectors listed by Kjaerland are Com and Gov (Kjaerland 2006).

Clive Blackwell also extended Howard and Longstaff's taxonomy in 2010. This extension focused on the defensive posture of the victim of an attack. Where Howard and Longstaff focused on the objectives of the attacker, Blackwell attempts to understand the ultimate effect on the target (Blackwell 2010).

Blackwell makes several significant changes to the terminology used by Howard and Longstaff. Blackwell uses the term *perpetrator* rather than *attacker* in order to differentiate between intended and unintended consequences. According to Blackwell, an attacker always intends to cause harm where a perpetrator may not be intending to cause harm, but harm may be caused by external factors (Blackwell 2010).

Blackwell also adapts the concept of an event. Rather than tying an incident to a single event, Blackwell ties an incident to stages that may be composed of one or more events with a common purpose. This concept of stages also allows Blackwell to account for the different parts of an incident. These parts include "accessing the system, using the targeted resource, and escaping without detection" (Blackwell 2010).

The next modification proposed by Blackwell is to use the term *method* rather than *tool*. By using the term *method*, Blackwell is able to account for the knowledge and abilities of the perpetrator along with the actual tools that were used. This term is complementary with Kjaerland's use of the term *"Method of Operation* (Blackwell 2010; Kjaerland 2006).

Blackwell also differentiates between the immediate effect of an attack and the ultimate effect. This is an important distinction because the long-term effects of an attack are often more serious than the immediate effect (Blackwell 2010).

Blackwell goes on to describe the defensive posture of the victim of an attack and how it relates to the attacker. Table 2-1 presents Blackwell's comparison of offensive and defensive categories as they relate to an incident (Blackwell 2010).

Table 2-1: Blackwell's Comparison of Offensive and Defensive Categories

Offensive Categories	Defensive Categories
Perpetrator	Defender and third party victim
Objective	Positive objective to achieve goals Negative objective to avoid incidents
Method	Positive method and negative control
Threat	Vulnerability
Agent	Employee or service provider
Action	Positive action and control reaction
Immediate target	Immediate target
Immediate effect	Immediate effect
Intended ultimate target	Ultimate affected target valuable to the defense
Ultimate effect for perpetrator	Ultimate effect on defender and third party victims

Kjaerland's taxonomy was used in creating a survey of attacks against Critical Infrastructure in 2012 (Miller and Rowe 2012). This effort brought to light some of the challenges of using these types of taxonomies to describe incidents within a CPS.

A different approach to creating a taxonomy was taken by Hansman and Hunt. In this taxonomy, attacks are classified in four dimensions. The first dimension classifies the attack vector. The attack vector is the means by which an attack is carried out. The basic attack vectors are defined as Virus, Worm, Trojan, Buffer Overflow, Denial of Service, Network Attack, Physical Attack, Password Attack, and Information Gathering Attack. These attack vectors can be further classified based on the specific methods utilized in the attack (Hansman and Hunt 2005).

The second dimension defined in this taxonomy describes the target of an attack. This dimension is broken down by hardware or software targets. Hardware targets are further described based on the type of hardware. This could include processors, network equipment, or peripheral devices. Software targets are classified as either Operating System or Application. These are further defined all the way down to specific versions of the software that was targeted (Hansman and Hunt 2005).

The third dimension covers the vulnerabilities and exploits that are used by the attack. The authors do not define the categories to be used in this dimension. Rather, the Common Vulnerabilities and Exposures (CVE) database is used for classification purposes ("CVE - Common Vulnerabilities and Exposures (CVE)").

The fourth dimension defined by Hansman and Hunt deals with payloads or effects beyond the initial attack vector. These are classified as payloads that are themselves a first dimension attack vector, corruption of information, disclosure of information, theft of service, or subversion. Other than payloads that are themselves an attack vector, the other categories were all previously defined by Howard and Longstaff. Hansman and Hunt admit that their taxonomy is not comprehensive and thus they allow for additions in any of the four domains they have specified. They also allow for more domains to be added as necessary (Hansman and Hunt 2005).

Another taxonomy was presented by Simmons et al. This taxonomy was given the name AVOIDIT based on its classification categories. These categories are Attack Vector, Operational Impact, Defense, Informational Impact, and Target. This taxonomy draws on many of the same concepts as Howard and Longstaff and Kjaerland. The author's stated goal is to develop "a complete useful taxonomy" (Simmons et al. 2009).

The Attack Vector as defined in the AVOIDIT taxonomy would more properly be labeled Exploited Vulnerability. The authors make no attempt to define how the attack was carried out. Rather, they are more interested in the vulnerabilities within the system that were exploited in the attack. The categories listed within Attack Vector include Misconfiguration, Design Flaws, Kernel Flaws, Buffer Overflow, Race Condition, and Incorrect Permission among others (Simmons et al. 2009).

The Operational Impact in the AVOIDIT taxonomy is a description of the methods used by the attacker. This class includes Misuse of Resources, User Compromise, Root Compromise, Web Compromise, Installed Malware, and Denial of Service. These categories are designed to be mutually exclusive and easily presented to and understood by the public (Simmons et al. 2009).

The Defense category defines the Mitigation and Remediation efforts a defender might employ both before and after an attack. The mitigation efforts refer to steps taken by a defender before an attack in an attempt to prevent a successful attack. The remediation efforts are those steps taken to correct the situation during or after an attack (Simmons et al. 2009).

Informational Impact refers to the impact an attack has on the informational aspects of a system. These impacts include Distort, Disrupt, Destruct, Disclosure, and Discovery.

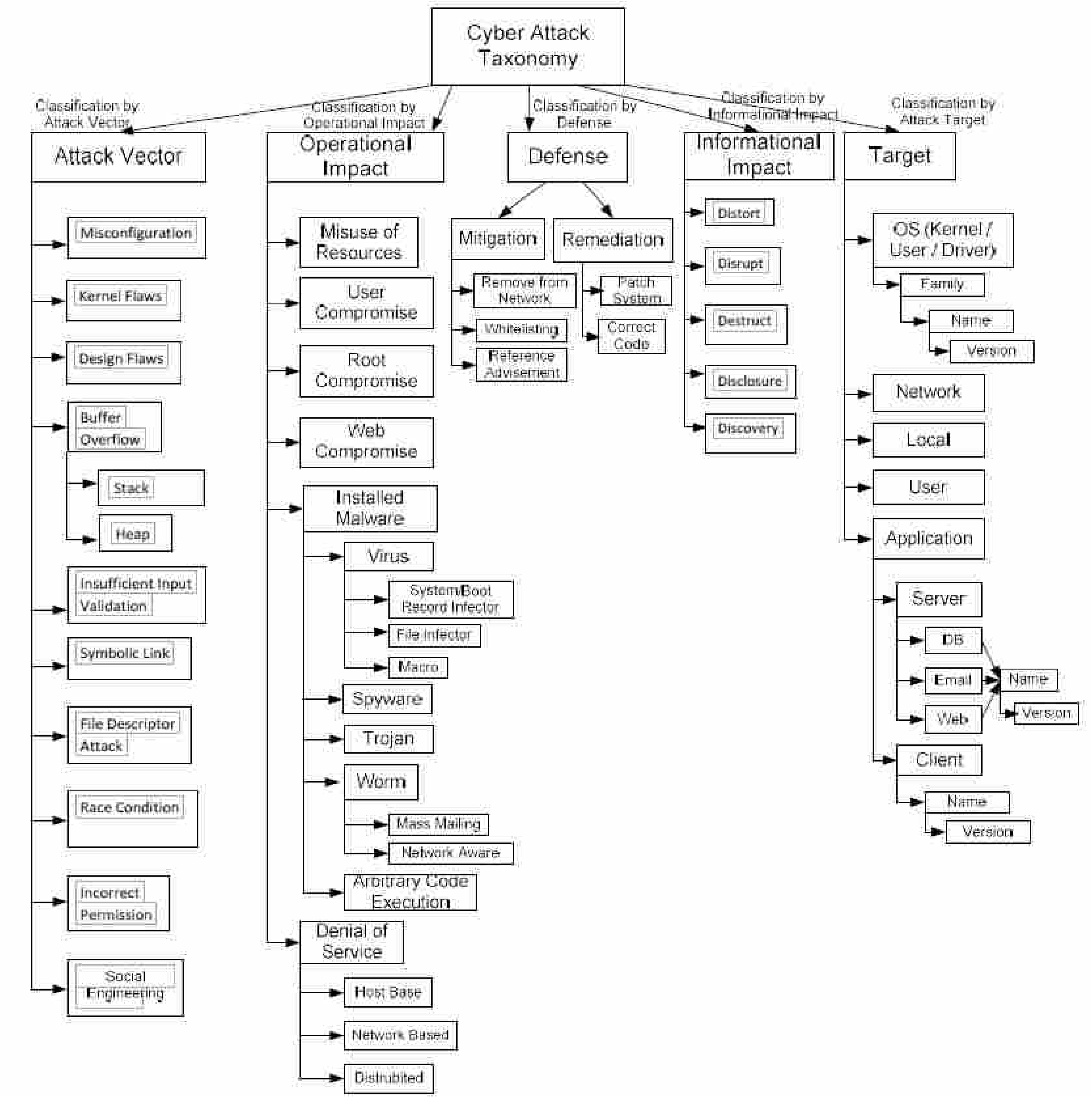


Figure 2-4: AVOIDIT Incident Taxonomy

The target of an attack, as defined by AVOIDIT, is where in the system the attack takes place. This could include the Operating System, Network, User, or Application. These different targets could leave a defender unknowingly susceptible to another attack. Figure 2-4 represents the AVOIDIT taxonomy (Simmons et al. 2009).

2.3.2 Specific Taxonomies

Aside from the general taxonomies, there are also taxonomies that deal with specific aspects of a cyber-attack. Some of these taxonomies focus on the type of system that is being attacked; others focus on the type of attack that is being carried out.

A taxonomy of cyber-attacks on SCADA systems was presented in 2011 (Zhu, Joseph, and Sastry 2011). This taxonomy describes some of the differences a SCADA system has from a typical IT network. Some of these differences include a difference in the priorities of system protection. In a SCADA system, integrity and availability are typically of greater concern than confidentiality. In a typical IT network, it is usually the central servers that are the primary concern in an attack, but in a SCADA system, the end nodes are of equal concern because this is where the physical aspects of the system are contained. There are also protocol differences that must be accounted for in an attack on a SCADA system (Zhu, Joseph, and Sastry 2011). While the title of the paper was "A Taxonomy of Cyber Attacks on SCADA Systems," an actual taxonomy was never presented.

Along with the taxonomies that focus on the type of system that is under attack, there are also taxonomies that deal with the type of attack being carried out. In 2003, a taxonomy was presented to detail attacks carried out utilizing computer worms. This taxonomy focused on five key attributes of computer worms. These areas are Target Discovery, Carrier, Activation, Payloads, and Attackers. Target Discovery defines how a worm identifies new targets for infection. The Carrier is the method the worm uses propagate onto a target. Activation describes how the worm begins operating on the target. Payloads are the non-propagating parts of the worm that carry out the attackers intended purposes. Attackers attempts to define the motives which drive the attackers and their choice of payloads (Weaver et al. 2003).

Another of this type of taxonomy attempts to describe Distributed Denial of Service (DDoS) attacks and defense mechanisms. This taxonomy defines DDoS attacks by Degree of Automation, Exploited Weakness to Deny Service, Source Address Validity, Attack Rate Dynamics, Possibility of Characterization, Persistence of Agent Set, Victim Type, and Impact on Victim (Mirkovic and Reiher 2004). Figure 2-5 illustrates the DDoS attack taxonomy.

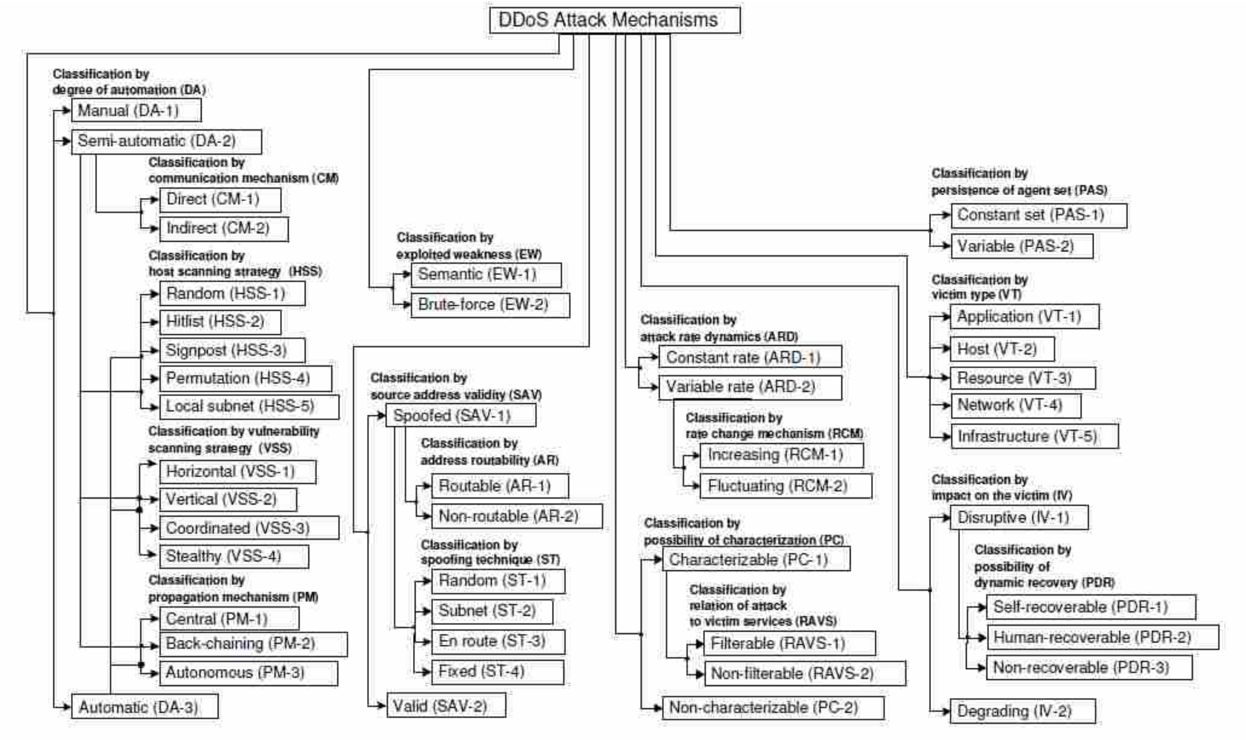

DDoS Attack Mechanisms
Classification by degree of automation (DA)
Manual (DA-1)
Semi-automatic (DA-2)
Classification by communication mechanism (CM)
Direct (CM-1)
Indirect (CM-2)
Classification by host scanning strategy (HSS)
Random (HSS-1)
Hitlist (HSS-2)
Signpost (HSS-3)
Permutation (HSS-4)
Local subnet (HSS-5)
Classification by vulnerability scanning strategy (VSS)
Horizontal (VSS-1)
Vertical (VSS-2)
Coordinated (VSS-3)
Stealthy (VSS-4)
Classification by propagation mechanism (PM)
Central (PM-1)
Back-chaining (PM-2)
Autonomous (PM-3)
Automatic (DA-3)
Classification by exploited weakness (EW)
Semantic (EW-1)
Brute-force (EW-2)
Classification by source address validity (SAV)
Spoofed (SAV-1)
Classification by address routability (AR)
Routable (AR-1)
Non-routable (AR-2)
Classification by spoofing technique (ST)
Random (ST-1)
Subnet (ST-2)
En route (ST-3)
Fixed (ST-4)
Valid (SAV-2)
Classification by attack rate dynamics (ARD)
Constant rate (ARD-1)
Variable rate (ARD-2)
Classification by rate change mechanism (RCM)
Increasing (RCM-1)
Fluctuating (RCM-2)
Classification by possibility of characterization (PC)
Characterizable (PC-1)
Classification by relation of attack to victim services (RAVS)
Filterable (RAVS-1)
Non-filterable (RAVS-2)
Non-characterizable (PC-2)
Classification by persistence of agent set (PAS)
Constant set (PAS-1)
Variable (PAS-2)
Classification by victim type (VT)
Application (VT-1)
Host (VT-2)
Resource (VT-3)
Network (VT-4)
Infrastructure (VT-5)
Classification by impact on the victim (IV)
Disruptive (IV-1)
Classification by possibility of dynamic recovery (PDR)
Self-recoverable (PDR-1)
Human-recoverable (PDR-2)
Non-recoverable (PDR-3)
Degrading (IV-2)

Figure 2-5: DDoS Attack Taxonomy

Every taxonomy contains strengths and weaknesses. Taxonomies are generally useful within the realm where they are designed to be used, but they present challenges when attempting to describe something that was not intended to be described by the taxonomy. This is the reason why all of these taxonomies have difficulties in describing incidents within a CPS. There are no currently available taxonomies to describe these types of incidents.

2.4 Examples of Incidents

Incidents such as the SQL Slammer worm infection at the Davis-Besse nuclear power plant and the Stuxnet attack on the Iranian nuclear facility at Natanz have made it clear that more needs to be done to protect our critical infrastructure. Most of the focus has been on Industrial Control Systems (ICS) particularly Supervisory Control and Data Acquisition (SCADA) systems. This is a reasonable place to start. There are, however, other incidents that have affected other areas within a CPS. A few examples of these types of incidents will be useful in understanding the relationship between incidents in the broader realm of CPSs.

2.4.1 Hospital Malware

Beth Israel Deaconess Medical Center in Boston has 664 pieces of medical equipment that run on older versions of the Microsoft Windows Operating System. The manufacturers of this equipment will not allow the hospital to modify the systems even to install anti-virus software because of disagreements over whether modifications could run afoul of U.S. Food and Drug Administration regulatory reviews. This equipment is often infected with malware, and one or two devices have to be taken out of service each week to be cleaned of these infections. These infections and the resultant down-time compromise the quality of care hospital patients receive. If the wrong piece of equipment were compromised at a critical time, the consequences could be disastrous (Talbot 2012).

2.4.2 Airport Hack

In March 1997, one hacker penetrated and disabled a telephone company computer that serviced Worcester Airport in Massachusetts. As a result, the telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service, and various private airfreight companies was cut off for six hours. Later in the day, the juvenile disabled another telephone company computer, this time causing an outage in the Rutland area. The outage caused financial losses and threatened public health and public safety (Denning 2000).

2.4.3 Pipeline Explosion

In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1½ hours after the rupture, the gasoline ignited and burned approximately 1½ miles along the creek causing three deaths and eight documented injuries. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. The National Transportation Safety Board (NTSB) report issued October 2002 cited one of the five key causes of the accident was the Olympic Pipe Line Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline (Tsang 2012).

2.4.4 Summary

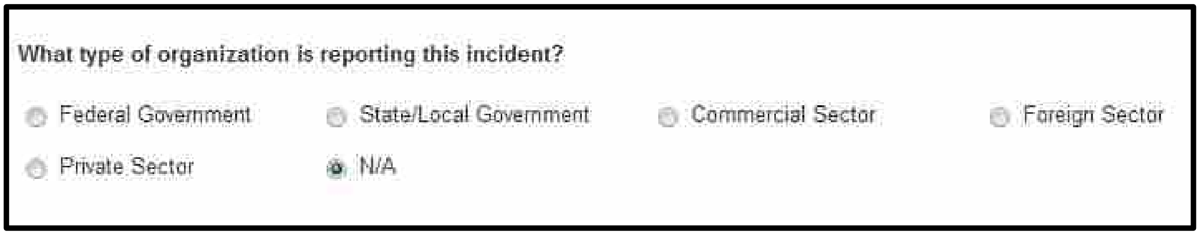
Each of these incidents has unique characteristics that set them apart from the others. They also have characteristics in common that can be compared and used to help prevent further incidents. The major characteristic each of these incidents has in common is the potential for impact on human lives. This potential to impact the physical world is one of the key features of cyber-physical systems.

2.5 Incident Repositories

A classification system is useful for providing a standardized method for studying an incident; this method, however, is not as useful as it could be if there is no way to compare incidents to find their similarities and differences. There are many incident databases available, but none of the currently available databases are useful for making this type of comparison. There are general incident databases that attempt to catalog all cyber-security incidents, but these databases do not contain the information that would be specific to CPSs, and many of them are no longer being updated (Sveen et al. 2007). There are also databases that detail security incidents relating only to specific systems.

2.5.1 General Repositories

An example of a general repository is the US-CERT database (US-CERT 2014). This database focuses more on vulnerabilities than incidents. This database has no regard for CPSs and considers a limited range of market sectors as can be seen in Figure 2-6. This database is also US centric with no discussion of incidents in other locations.



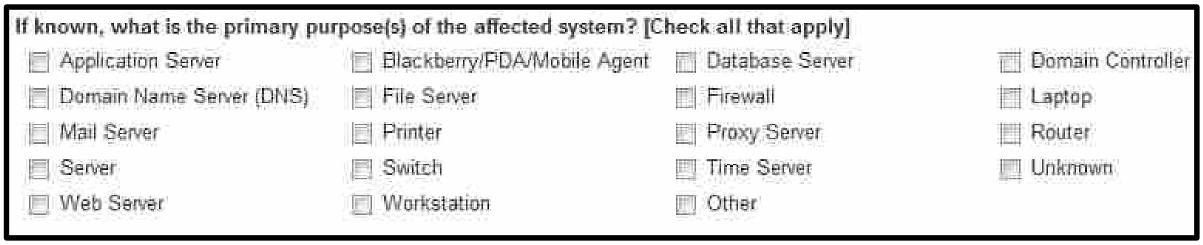
What type of organization is reporting this incident?

○ Federal Government ○ State/Local Government ○ Commercial Sector ○ Foreign Sector

○ Private Sector ● N/A

Figure 2-6: US-CERT Sectors

There are other issues with relying on the US-CERT database as a repository for CPS incidents. For example, when specifying the primary purpose of the affected system, only a limited range of options are available. These options are not updated for newer technologies. This limitation can be seen in Figure 2-7.



If known, what is the primary purpose(s) of the affected system? [Check all that apply]

□ Application Server
□ Blackberry/PDA/Mobile Agent
□ Database Server
□ Domain Controller
□ Domain Name Server (DNS)
□ File Server
□ Firewall
□ Laptop
□ Mail Server
□ Printer
□ Proxy Server
□ Router
□ Server
□ Switch
□ Time Server
□ Unknown
□ Web Server
□ Workstation
□ Other

Figure 2-7: US-CERT System Purposes

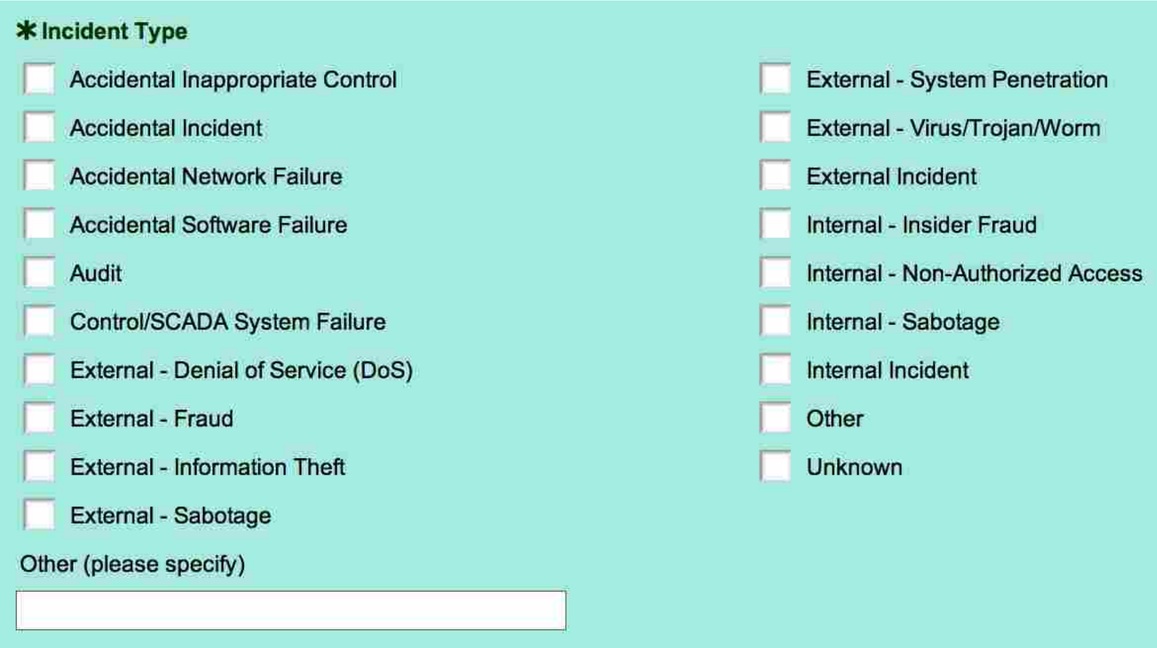
These issues, along with others, limit the usefulness of the US-CERT incident database for cataloging incidents relating to CPSs. There is a need for a repository that is focused on the unique aspects of CPSs and is international in scope.

2.5.2 Specific Repositories

There are also incident databases that focus on specific types of incidents. The main repository that relates to CPSs is the Repository of Industrial Security Incidents (RISI 2014). RISI is designed to “collect, investigate, analyze, and share important industrial security incidents among member companies so they can learn from experiences of others” (RISI 2014). RISI began as the Industrial Security Incident Database (ISID) in 2001. ISID was discontinued in 2006. In 2009, the Security Incidents Organization™ was created to operate RISI (RISI 2014).

RISI provides many of the classification categories that are needed to describe CPS incidents. For example, RISI provides classifications for Incident Type, Incident Perpetrator, Incident Results, Financial Impact, and Downtime. These categories can be seen in figures 2-8 through 2-12 (RISI 2014).

RISI has three general classifications for incident type. Each of these has multiple sub-classifications. The general classifications are Accidental, External, and Internal. RISI does not use a hierarchical selection for incident type; rather, the options are presented in a single list. These options can be seen in Figure 2-8.



✱ Incident Type

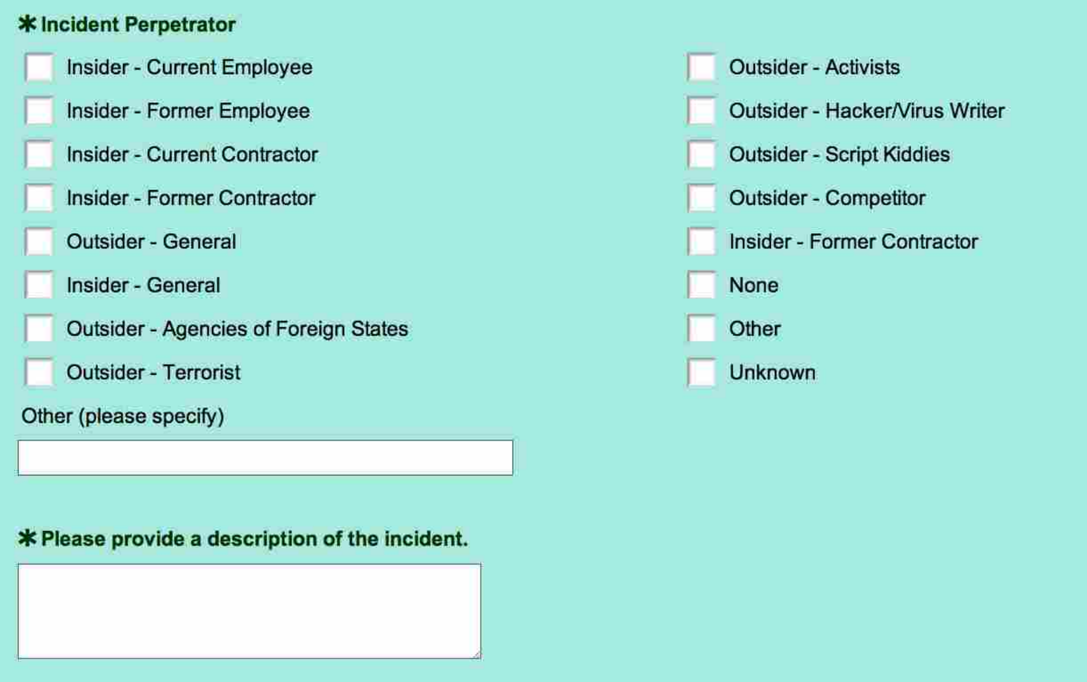
□ Accidental Inappropriate Control
□ Accidental Incident
□ Accidental Network Failure
□ Accidental Software Failure
□ Audit
□ Control/SCADA System Failure
□ External - Denial of Service (DoS)
□ External - Fraud
□ External - Information Theft
□ External - Sabotage
□ External - System Penetration
□ External - Virus/Trojan/Worm
□ External Incident
□ Internal - Insider Fraud
□ Internal - Non-Authorized Access
□ Internal - Sabotage
□ Internal Incident
□ Other
□ Unknown

Other (please specify)

Figure 2-8: RISI Incident Types

As can be seen, the Accidental incident types refer mainly to component failures and other incidental events. The External incident types are more closely related to the incident means or attacks as referred to in the available taxonomies. The Internal incident types refer to malicious behavior by an internal employee. There are also options for Audit, Control System Failure, Other, and Unknown incidents.

The Incident Perpetrator, as defined by RISI, contains Insider and Outsider perpetrators. As with the incident type, each of these has several sub-classifications. These options can be seen in Figure 2-9.



✱ Incident Perpetrator

□ Insider - Current Employee
□ Insider - Former Employee
□ Insider - Current Contractor
□ Insider - Former Contractor
□ Outsider - General
□ Insider - General
□ Outsider - Agencies of Foreign States
□ Outsider - Terrorist

□ Outsider - Activists
□ Outsider - Hacker/Virus Writer
□ Outsider - Script Kiddies
□ Outsider - Competitor
□ Insider - Former Contractor
□ None
□ Other
□ Unknown

Other (please specify)

✱ Please provide a description of the incident.

Figure 2-9: RISI Incident Perpetrators

The Incident results portion of RISI is a selection list of results from the perspective of the entity where the incident occurred. The Incident results include options for equipment damage or loss, loss of time in both production and staff time, theft of intellectual property, public effects (both human and property), monetary damages (fraud or fines), and communication failures. These results can be seen in Figure 2-10.

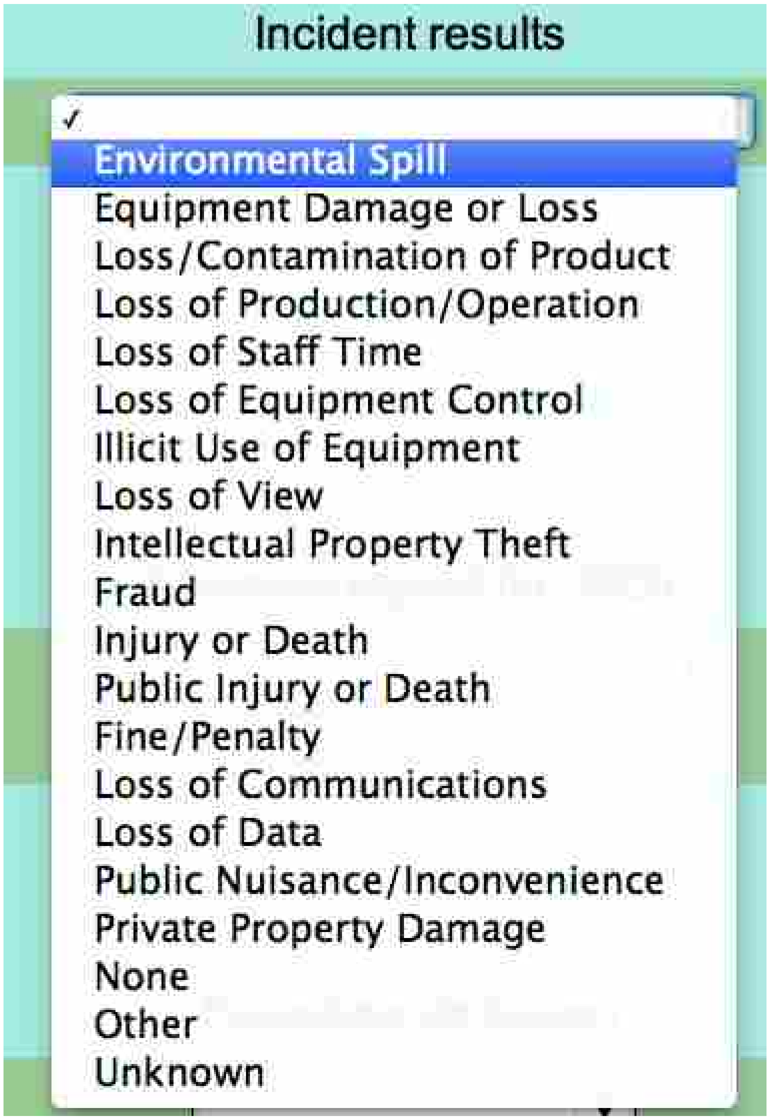


Figure 2-10: RISI Incident Results

The financial impact as reported in RISI is a range in US dollars. It is not clear whether this impact is just for the entity where the incident occurred, or if it includes financial impacts to other entities. This can be seen in Figure 2-11.

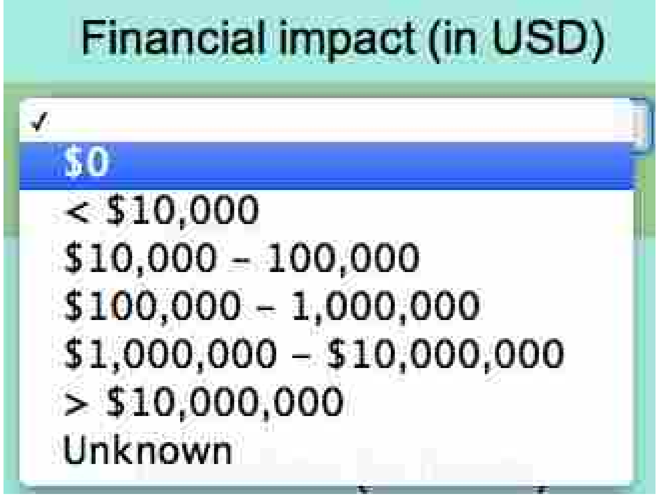


Figure 2-11: RISI Financial Impact

The downtime as reported in RISI is in ranges of hours. This could be from zero downtime to greater than 72 hours. This is shown in Figure 2-12.

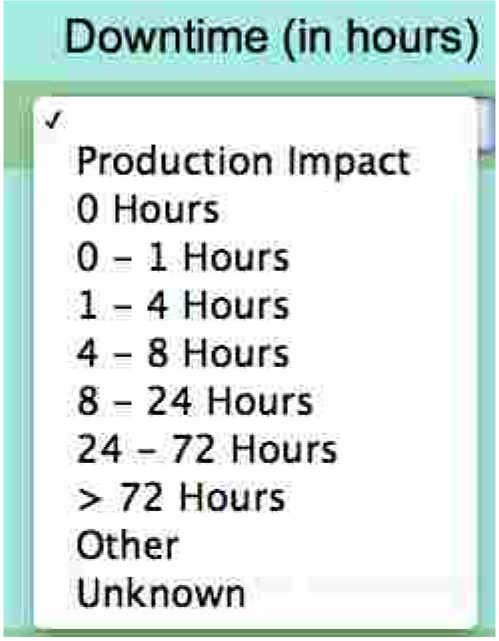


Figure 2-12: RISI Downtime

As with US-CERT, there are some problems with RISI as it relates to CPSs. RISI is focused on Industrial Control Systems. These systems are a critical piece of the CPS space, but there are many other types of systems within the CPS realm that are not accounted for by RISI. RISI is also designed for use by members of industry. As such, RISI charges thousands of US dollars per year for access to the repository. This is problematic when attempting to find information about these types of incidents for other types of research.

The issues with US-CERT and RISI demonstrate the need for a new incident repository that is focused on CPS incidents. This repository should allow for cross-domain analysis of incidents and should be freely available for academic research to take advantage of the benefits obtainable from collaboration between a wide and diverse pool of researches and cyber-security professionals.

2.6 Chapter Summary

There are many conflicting definitions of what constitutes a CPS. These ideas range from large scale industrial control systems to small systems such as smart phones or tablets. The best way to describe a CPS is to focus on the shared characteristics. In its simplest form, a CPS can generally be considered to be the interface between the cyber world and the physical world.

There have been many attempts at creating a taxonomy to describe cyber-security incidents. These taxonomies may focus on how the incident was carried out, how the incident was defended against, or what the impact of the incident was. All of the existing taxonomies have weaknesses when trying to describe incidents within CPSs. There is a need for a new taxonomy that accounts for the unique characteristics of CPSs and the challenges that CPSs present.

Attempts have also been made in creating incident repositories to allow for the study of cyber-security incidents. These repositories face some of the same challenges with CPSs as the incident taxonomies. In addition to the difficulties of accounting for the unique characteristics of CPSs, some of these repositories cost a significant amount to be able to access and are not available for academic research.

The challenges presented by CPSs along with the lack of currently available taxonomies and incident repositories are a hindrance for researchers attempting to study these types of security incidents and find better methods of protection to avoid incidents in the future. A cross domain, impact oriented classification system and database are needed to facilitate better research into the nature and impact of these types of incidents.

3 METHODOLOGY

3.1 Introduction

This research will produce a framework for studying CPS incidents. This framework will also be used to answer the research questions and test the hypotheses presented in Chapter 1. This framework will consist of an incident taxonomy, a reporting workflow, a website and a database. A validation study will also be conducted as part of this research. Using the framework as part of the research will allow the research questions to be answered and the hypotheses to be tested within the context in which they are intended to be used long term.

3.2 Taxonomy Categories

Q1 “What taxonomy categories will allow for cross domain analysis of incidents?” and Q2 “What taxonomy categories will allow for an impact oriented analysis of incidents?” shall be answered as follows. A working group of CPS and cyber-security researchers shall be formed. This group will provide an initial Delphi study using a modified version of Kjaerland’s taxonomy (Miller and Rowe 2012) as a starting point to define the categories necessary for an incident taxonomy that focuses on CPSs. This initial taxonomy is presented in Table 3-1.

Table 3-1: Initial Taxonomy

Source Sectors	Method of Operation(MO)	Impact	Target Sectors
Com	Misuse of Resources	Disrupt	Com
Gov	User Compromise	Distort	Gov
Edu	Root Compromise	Destruct	Intl
Intl	Social Engineering	Disclosure	
User	Virus	Death	
Unknown	Web Compromise	Unknown	
	Trojan		
	Worm		
	Recon		
	Denial of Service		
	Other Sys Failure		

The group will develop a list of categories that are required for a taxonomy that describes CPS incidents.

3.2.1 Taxonomy Refinement

After the initial taxonomy is created, it will be presented to the steering group for further refinement and clarification. The group will utilize an affinity diagram technique to analyze and categorize comments on the taxonomy. The results of that exercise will then be used to create the final taxonomy.

3.3 Methods for Measuring Impact

H1 “Suitable methods for measuring the impact of an incident currently exist.” shall be tested through a literature survey to identify current methods for measuring the impact of an incident. This survey will not be limited to cyber-security methods for measuring impact, but will also draw from other disciplines. H2 “Currently available methods can be adopted for use in CPS incidents.” shall be tested through the taxonomy refinement process already described.

3.4 Identifiable Benefits

Q3 “What are the identifiable benefits of a cross domain classification system?” and Q4 “What are the identifiable benefits of an impact oriented classification system?” shall be answered as follows. The identifiable benefits of this method of classification will be determined by using the taxonomy to classify several incidents. This will be done through the creation of a database of incidents. The database will be created to follow the specifications of the incident taxonomy.

Several incidents will then be added to this database with their classifications. These incidents will be gathered using a literature survey. Incidents involving a CPS will be selected from incident reports in academic publications, news outlets, and other information sources.

The final taxonomy will be compared to other currently existing taxonomies. This comparison will be made using the incidents that are included in the database. Each incident will be classified using the taxonomy presented here along with several currently existing taxonomies. The results of this comparison will identify the benefits of utilizing a cross-domain impact-oriented taxonomy for classifying incidents within a CPS.

This comparison will involve analyzing the results of the classification in different taxonomies to identify benefits and weaknesses of the presented taxonomy.

3.5 Organization of Results

The results of this work will be presented in the following chapters. Chapter 4 will document the evolution of the incident taxonomy. In Chapter 5, the entire proposed framework will be presented along with analysis and observations for each of the framework components. Chapter 6 will present conclusions drawn from this research along with recommendations for future work.

3.6 Validation of Results

The results will be validated utilizing the process illustrated in Figure 3-1. Several incidents will be used to validate the results. Each incident will be discussed. A classification based on the current taxonomy will be proposed. The classification will be validated, and the taxonomy will be improved as needed.

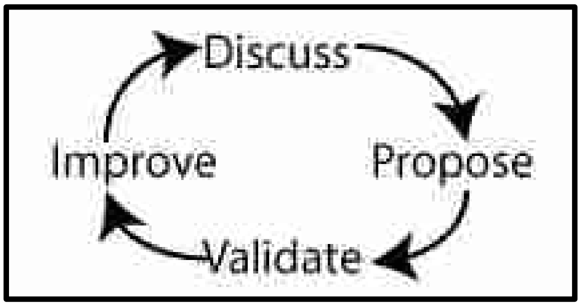


Figure 3-1: Results Validation Process

Eight different incidents will be used in the validation process. Each incident will be classified using the newly developed taxonomy along with Howard and Longstaff's taxonomy, Kjaerland's taxonomy, and the AVOIDIT taxonomy. An introduction to the eight incidents will be given here. The results of the classification exercise will be provided in Chapter 5.

3.6.1 Hospital Malware

Beth Israel Deaconess Medical Center in Boston has 664 pieces of medical equipment that run on older versions of the Microsoft Windows Operating System. The manufacturers of this equipment will not allow the hospital to modify the systems even to install anti-virus software. This equipment is often infected with malware, and one or two devices have to be taken out of service each week to be cleaned of these infections. These infections and the resultant down-time compromise the quality of care hospital patients receive. If the wrong piece of equipment were compromised at a critical time, the consequences could be disastrous (Talbot 2012).

3.6.2 Airport Hack

In March 1997, one hacker penetrated and disabled a telephone company computer that serviced Worcester Airport in Massachusetts. As a result, the telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service, and various private airfreight companies was cut off for six hours. Later in the day, the juvenile disabled another telephone company computer, this time causing an outage in the Rutland area. The outage caused financial losses and threatened public health and public safety (Denning 2000).

3.6.3 Pipeline Explosion

In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1½ hours after the rupture, the gasoline ignited and burned approximately 1½ miles along the creek causing three deaths and eight documented injuries. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. The National Transportation Safety Board (NTSB) report issued October 2002 cited one of the five key causes of the accident was the Olympic Pipe Line Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline (Tsang 2012).

3.6.4 Maroochy Water System

In Maroochy Shire, Queensland, Australia in 2000 a disgruntled ex-employee hacked into a water control system and flooded the grounds of a hotel and a nearby river with over 264,000 gallons of raw sewage. The Maroochy Shire attack was not one attack but a whole series of attacks over a prolonged period (Mustard 2005).

3.6.5 Train System Virus

In 2003, a computer virus named Sobig was reported to have shut down train signaling systems in Florida, U.S. The virus was reported to have been one of the fastest spreading e-mail attachment viruses at the time. It shut down the signaling, dispatching, and other systems at CSX Corporation; one of the largest transportation suppliers in the U.S. While there were no major incidents caused by this case, many trains were delayed (Nicholson et al. 2012).

3.6.6 Nuclear Power Plant Worm

The SQL Slammer Worm began infecting systems in January 2003. At this time, the worm infected the network of a contractor doing work for the Davis-Besse Nuclear Power Plant. The worm spread through a T1 line between the contractor and the power plant’s business network. This T1 line bypassed the plant’s firewalls. From the business network, the worm spread to the plant’s control network and infected at least one unpatched server. The worm created network congestion which caused the plant’s Safety Parameter Display System to crash (Poulsen 2003).

3.6.7 Stuxnet

In June 2010, it was discovered that a worm dubbed Stuxnet had struck the Iranian nuclear facility at Natanz. Stuxnet used four ‘zero-day vulnerabilities’ (vulnerabilities previously unknown, so there has been no time to develop and distribute patches). The worm employs Siemens' default passwords to access Windows operating systems that run specific SCADA programs. The worm would hunt down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland. These drives were used to power centrifuges used in the concentration of the uranium-235 isotope. Stuxnet altered the frequency of the electrical current to the drives causing them to switch between high and low speeds for which they were not designed. This switching caused the centrifuges to fail at a higher than normal rate (Farwell and Rohozinski 2011).

3.6.8 Cellular Network Vehicle Attack

Researchers from the University of Washington and the University of California San Diego were able to demonstrate the capability of using the cellular network to attack vehicle telematics systems such as GM's OnStar or Ford's Sync (Checkoway et al. 2011).

3.7 Production of Database

A database of incidents shall be developed as part of this research. This database will be used to aid in the validation of the results. The database will be designed to allow incidents to be classified according to the initial taxonomy. As the results are validated and the taxonomy is improved, the database will be modified to follow the changes made to the taxonomy. At the conclusion of this research, the database will be made available through a website for academic research into CPS incidents.

3.8 Chapter Summary

The framework that will be developed as part of this research will be used to determine the best methods for describing incidents within CPSs. This framework will also be used to create an incident repository that will be available for academic research into the methods and impacts of these incidents. This framework will allow us to define the necessary categories for incident classification, methods for measuring the impact of an incident, and the benefits of this type of classification.

4 TAXONOMY EVOLUTION

4.1 Introduction

This chapter will present how the CPS incident taxonomy evolved from a taxonomy used to describe incidents in SCADA and critical infrastructure systems to one that may be used to describe an incident in any CPS. An analysis of how the taxonomy will achieve this goal will also be presented.

4.2 Initial Taxonomy

The initial taxonomy was a modification of Kjaerland's taxonomy that was used to conduct a survey of critical infrastructure incidents (Miller and Rowe 2012). The modifications to Kjaerland's taxonomy include adding Other Sys Failure to the Methods of Operation, Death to the Impact, and Intl to the Target Sectors. These modifications were made in an attempt to account for the CPS factors inherent in critical infrastructure and SCADA systems. This initial taxonomy is presented in Table 4-1.

Table 4-1: Initial Taxonomy

Source Sectors	Method of Operation (MO)	Impact	Target Sectors
Com	Misuse of Resources	Disrupt	Com
Gov	User Compromise	Distort	Gov
Edu	Root Compromise	Destruct	Intl
Intl	Social Engineering	Disclosure	
User	Virus	Death	
Unknown	Web Compromise	Unknown	
	Trojan		
	Worm		
	Recon		
	Denial of Service		
	Other Sys Failure		

4.3 Evolution

The categories as initially defined were Source, Means, Market Sector, Impact, and Criticality. These categories were then used to create a taxonomy which was brought back to the group for further refinement and clarification.

Each of the taxonomy categories was defined as follows.

The Source of an incident was defined as where the incident originated. The source was divided into six possible classifications. These classifications were Commercial, Government, Educational, Organization, Individual, and Unknown.

The Means of an incident defined how the incident occurred. The classifications for means were Misuse of Resources, User Compromise, Root Compromise, Social Engineering, Virus, Web Compromise, Trojan, Worm, Recon, Denial of Service, and Other System Failure.

The Market Sector was used to describe the victim of an incident. This category defined the market a victim primarily does business in. The defined Market Sectors were Utilities, Industrial Process Control, Health Care, Transportation, Aerospace, Military, Consumer

Electronics, Facilities Infrastructure, Agriculture, Physical Access Control, Communications, Construction, and Media Creation and Distribution.

The Impact category was used to define the effects of the incident on the victim. The classifications to define Impact were Disrupt, Distort, Destroy, Disclose, Death/Serious Injury, and Unknown.

The Criticality of an Incident was meant to describe how severe the Incident was. The Criticality was broken into five different classifications. These classifications were Inconvenience, Secondary Operations Affected, Primary Operations Affected, Primary Operations Halted, and Human Life Affected.

These definitions were taken back to the research group for further discussion and refinement. The group performed a sticky note exercise where each member of the group was given a unique color of sticky notes. Each member of the group was then given an opportunity to examine each of the categories and write any comments they had on one of their sticky notes and attach it to the category. Each of the comments was reviewed as a group after each member was given an opportunity to review each of the categories. This review of the comments was then used to make modifications to the taxonomy.

4.4 Cross-Domain Analysis

During the process of classifying incidents, it was discovered that many incidents involved multiple means and target market sectors. This discovery led to the creation of a taxonomy that allows for multiple classification capabilities. The ability to classify an incident multiple times in each taxonomy category became a necessary feature of the framework due to this discovery. The multiple classification of target market sectors also provides the ability for cross domain analysis of incidents utilizing this framework.

4.5 Analysis of Findings

Several taxonomy categories were defined that allow for cross domain and impact oriented analysis of incidents. The categories that are required for cross domain analysis are Victim Type and Victim Market Sector. The Victim Type allows for a correlation of the general features of a victim of a CPS incident. The victim Market Sector gives the ability to identify the interactions between the sectors and how a single incident may involve multiple domains.

The categories that are necessary to conduct an impact oriented analysis of incidents are Direct Impact and Indirect Impact with Impact Severity, Immediacy of Impact, Recovery Time, and Monetary Impact as modifiers. The direct and indirect impact categories provide a view into the impacts of an incident on the system and the surrounding environment. The modifiers provide a method for comparing these impacts across incidents.

In the creation of the new taxonomy, different methods for measuring the severity of impacts were consulted. These methods were drawn from health care, information assurance and security, and physical security industries. Most methods of measuring severity relied on a scale of severity. This scale is typically a Low/Medium/High severity scale. An example of this would be the OWASP Risk Rating Methodology (OWASP). This scale was modified to provide severity for primary and secondary operations.

The final proposed taxonomy is presented in Chapter 6.

4.6 Chapter Summary

The proposed taxonomy began as an attempt to describe incidents within SCADA and critical infrastructure systems. The taxonomy was modified and refined through an iterative process of making changes and attempting to classify several CPS incidents to find flaws and weaknesses. The taxonomy was then updated to correct these flaws and weaknesses and several more incidents were classified using the new taxonomy. This process was repeated until the taxonomy could be used to describe any CPS incident that was attempted. This process identified the categories that are required to describe a CPS incident along with a method for describing the impact of an incident.

5 PROPOSED FRAMEWORK

5.1 Introduction

The incident taxonomy is just one piece of what is needed to be able to study incidents within CPSs. The taxonomy is one piece of a larger framework that is necessary for this type of analysis. In this chapter, the entire framework will be presented beginning with the complete taxonomy. This framework also includes an incident database and workflow along with a website that will be used to make information about these incidents available to those who are studying them.

5.2 BYU-CPS Incident Taxonomy

The final taxonomy as developed after the research group made comments and suggestions on the initial taxonomy is presented here. The taxonomy has been designated the BYU-CPS Incident Taxonomy. This taxonomy includes four main categories with sub-classifications and modifiers to provide further detail. The four main categories are Source Type, Means, Impact, and Victim. Each of these categories will be presented in further detail here.

5.2.1 Source Type

The Source Type of an incident describes the general features of the entity where an incident originated. The Source Type is designed to group incidents into general classes by where they were initiated. This type of classification will allow for analysis and understanding of the origin of incidents. The available Source Types are Commercial, Government, Educational, Non-Profit Organization, Individual, Identified Group, and Unknown.

Commercial – A Commercial source type would denote that the incident originated with a business entity of some type. The Commercial source type includes retail, manufacturing, industrial, and service enterprises along with similar entities. No consideration is given to the size of a commercial source.

Government – A Government source type would indicate an incident originated with some form of national or local government.

Educational – An Educational source type would be used to describe an incident that began in any type of educational institution. This could include academic research conducted at an institute of higher education, or it may be an incident that originated at any level of educational institution.

Non-Profit Organization – A Non-Profit Organization source type would be appropriate for any registered non-profit organization. This would exclude commercial and government institutions along with any unofficial entity.

Individual – An Individual source type is used if an incident is initiated by a single individual. This individual could be a legitimate user of the affected system or it could be some form of outside intruder.

Identified Group – An Identified Group source type would indicate some sort of identifiable conglomeration that is not an official entity. This would include hacktivist groups like Anonymous. It could also indicate an identified terrorist organization.

Unknown – An Unknown source type would be used for incidents where the source of the incident cannot be identified.

5.2.2 Means

The Means category is used to indicate how an incident occurred. In the case of a deliberate attack, the Means would indicate the methods used by the attacker. It would also describe what went wrong in the case of an unintentional failure. This category is not restricted to one option. An incident can have as many means as are necessary to describe what happened.

The available classifications within the Means category are Misuse of Resources, User-level Resource Compromise, Root-level Resource Compromise, Social Engineering, Virus, Web-site Compromise, Trojan, Worm, Recon, Denial of Service, and Other System Failure. Each of these classifications will be described here.

Misuse of Resources – The Misuse of Resources classification would be used to indicate an incident that occurred due to the inappropriate use of system resources. This could include the use of IT resources in a way that was not intended, such as the storing of unauthorized files. This could also indicate authorized use of the system in a way that is not advisable, such as doing software testing on a production system.

User-level Resource Compromise – A User-level Resource Compromise indicates that an unauthorized user gained access to standard user resources on a system. Examples would include an attacker compromising a user account on a system or a former employee utilizing improperly terminated credentials to access a system they are no longer authorized to access.

Root-level Resource Compromise – A Root-level Resource Compromise consists of gaining unauthorized access to administrator level privileges on a system. An example would be a valid user of a system performing an unauthorized privilege escalation to gain access to administrator resources on a system.

Social Engineering – Social Engineering consists of using human interactions rather than computer based operations to gain unauthorized access to a system. An example would be learning details about an authorized user of a system in order to be able to guess the passwords that individual uses on the desired system.

Virus – A virus is a piece of computer code that attaches itself to other processes in order to gain access to carry out functions that would not normally be available to it.

Web-site Compromise – A Web-site Compromise takes advantage of vulnerabilities within a web-site in order to gain access to the underlying system. A web-site compromise would typically be an early step in gaining access to resources where other means could be used to further an attack.

Trojan – A Trojan is a computer program that adds subversive elements to other computer programs. A trojan could be used to copy sensitive data off of a system or to maintain unauthorized access to a system that has already been compromised.

Worm – A Worm is similar to a Virus in that it attaches itself to other programs in order to gain access to typically unavailable functions. The difference between a worm and a virus is in the method of propagation. A worm has the capability of automatically seeking out and infecting new targets, while a virus must rely on a user to propagate to other systems.

Recon – Recon is the act of scanning or probing a system to see what services are available or what vulnerabilities might exist. Recon is usually a preliminary step to other methods of intrusion, but the recon itself can sometimes cause an incident to occur.

Denial of Service – A Denial of Service occurs when normal use of the system is limited or halted. This may occur when a service is crashed or hung due to flaws in the way the service operates. A denial of service may decrease access to a particular service or to an entire system.

Other System Failure – The Other System Failure classification would indicate that an incident was caused due to a design flaw or other failure in the system. It could be due to the failure of a component in the system, a system that was not designed for the proper capacity, or any other failure that is not covered in one of the other classifications.

5.2.3 Impact

The impact of an incident describes what effect the incident had on the system or surrounding environment. This category is designed to describe the effect of an incident on the computer system, the physical system, the organization, and the community where the incident occurred. The Impact is further divided into Direct and Indirect Impacts. The Severity of an Impact is also considered. There are also modifiers for the Impact to describe the Immediacy of Impact, Recovery Time, and Monetary Impact of an incident.

5.2.4 Direct Impact

The Direct Impact of an incident describes the tangible effects of an incident. The Direct Impact is designed to show the results of an incident on the system and surrounding environment. The classifications for Direct Impact are Service Disruption, Information Distortion, Physical Destruction, Environmental Destruction, Information Destruction, Information Disclosure, Death/Serious Injury, and Unknown.

Service Disruption – A Service Disruption indicates a disturbance in the normal operations of a system. This would include a change in access to the system or a deviation from the normal operating conditions of the system.

Information Distortion – Information Distortion indicates a corruption of the data that is stored within a system or the data that is acquired from the system. This could include the inappropriate modification of file contents or a system reporting conditions other than those that are actually present.

Physical Destruction – Physical Destruction occurs when an entire system or individual components within the system fail to operate or are damaged physically. This would indicate an incident caused a failure within the physical components of the system.

Environmental Destruction – Environmental Destruction indicates some sort of destruction to the physical environment in which the system resides. This would include air pollution, water pollution, or other types of environmental damage.

Information Destruction – Information Destruction is the deletion of information or files from a system. This loss of information may lead to other types of impacts.

Information Disclosure – Information Disclosure is the unauthorized exposure of information. This would include information about a system or information acquired from the system.

Death/Serious Injury – The Death/Serious Injury classification indicates an incident caused harm to human life.

Unknown – The Unknown classification is used when the Direct Impact of an incident cannot be determined.

5.2.5 Indirect Impact

The Indirect Impact of an incident includes those impacts that may not be noticeable at first. In many cases, the indirect impact of an incident will be longer lasting than the direct impact. The classifications within Indirect Impact are Loss of Reputation, Loss of Trust, Lost Business, Political Repercussions, and Public Response.

Loss of Reputation – Loss of Reputation would indicate that the public image of an incident's victim has been tarnished.

Loss of Trust – Loss of Trust occurs when external entities no longer believe in a victim's ability to operate in a safe and effective manner.

Lost Business – Lost Business indicates an impact on the ability of an incident's victim to do business. This impact is realized either through an inability to provide or a reduction of clients and orders based on the incident.

Political Repercussions – Political Repercussions may come about due to an incident. These may include increased regulation, reduction of tax benefits, or other impacts that come as a result of political processes.

Public Response – Public Response is indicated when the general public responds against an entity as a result of an incident. Public Response may include boycotts, demonstrations, or other actions taken by general members of the public.

5.2.6 Severity of Impact

The Severity of Impact is designed to indicate the magnitude of the impact of an incident on the system. The severity is a modifier to the direct impact on a system. The classifications within Severity of Impact are Inconvenience, Secondary Operations Degraded, Secondary Operations Halted, Primary Operations Degraded, and Primary Operations Halted.

Inconvenience – An Inconvenience indicates that an incident caused a minor disturbance but did not have a measurable effect on any operations of the system.

Secondary Operations Degraded – The Secondary Operations Degraded classification would be applied when operations that are ancillary to the primary function of a system are not functioning at normal levels.

Secondary Operations Halted – The Secondary Operations Halted classification would indicate that those ancillary functions have ceased entirely.

Primary Operations Degraded – Primary Operations Degraded would indicate that the primary function of a system is not being performed at normal levels.

Primary Operations Halted – Primary Operations Halted would indicate that an incident has completely debilitated a system's ability to perform its primary function.

5.2.7 Immediacy of Impact

The Immediacy of Impact of an incident is an indicator of how it takes for the impact to be recognized after an incident occurs. The immediacy of impact could be measured in seconds, minutes, hours, days, or any other unit of time. The immediacy of impact does not denote an increasing or decreasing scale of impact. Rather, it is a modifier of the impact to allow for a better understanding of how long it takes to for the impact of an incident to be discovered.

5.2.8 Recovery Time

The Recovery Time of an incident is another modifier of the impact. As with the immediacy of impact, the recovery time may be measured in any unit of time. A longer recovery time would indicate a greater degree of impact on a system.

5.2.9 Monetary Impact

The Monetary Impact of an incident is a measure of the cost of the incident to the victim. The monetary impact is another modifier to the impact of the incident. It is an attempt to determine both the hard recovery costs of an incident as well as the soft costs of lost revenues. Other factors to the monetary impact may include fines and increased taxes.

5.2.10 Victim

The Victim of an incident denotes where an incident occurs. The victim may be the target of a purposeful attack, or it may be the entity where an accident or failure occurs. The victim is described in two ways. First, the victim is described by Victim Type. Second, the victim is described according to the Market Sector which is impacted by the incident.

5.2.10.1 Victim Type

The Victim Type is similar to the Source Type category. The victim type is a general description of the features of the entity where the incident occurs. The classifications within Victim Type are the same as for Source Type.

Commercial – A Commercial victim type would denote that the incident occurred within a business entity of some type. The commercial victim type includes retail, manufacturing, industrial, and service enterprises along with similar entities. No consideration is given to the size of a commercial victim.

Government – A Government victim type would indicate an incident occurred within some form of national or local government.

Educational – An Educational victim type would be used to describe an incident that affected any type of educational institution. This could include academic research conducted at an institute of higher education, or it may be an incident that occurred at any level of educational institution.

Non-Profit Organization – A Non-Profit Organization victim type would be appropriate for any registered non-profit organization. This would exclude commercial and government institutions along with any unofficial entity.

Individual – An Individual victim type is used if an incident impacts a single individual.

Identified Group – An Identified Group victim type would indicate some sort of identifiable conglomeration that is not an official entity.

Unknown – An Unknown victim type would be used if the location of an incident cannot be identified.

5.2.10.2 Victim Market Sector

The Victim Market Sector is an attempt to identify the characteristics of the victim based on the usage of CPSs. These market sectors have been identified based on general characteristics of how CPSs are utilized within each sector. A victim may be classified in multiple market sectors. The identified Victim Market Sectors are Utilities, Industrial Process Control, Health Care, Transportation, Aerospace, Military, Consumer Electronics, Facilities Infrastructure, Agriculture, Physical Access Control, Communications, Construction, and Entertainment Media Creation and Distribution.

Utilities – The Utilities market sector is used to describe entities that are involved with the production and distribution of energy; collection, treatment, and distribution of water; and collection, treatment, and disposal of sewage among other activities.

Industrial Process Control – The Industrial Process Control market sector is concerned the oversight of industrial processes. This might include manufacturing, chemical production, and other similar activities.

Health Care – The Health Care market sector provides for medical diagnosis and treatment along with patient care. This sector encompasses hospitals, clinics, offices, and home health care.

Transportation – The Transportation market sector is involved in the movement of people and goods. This includes air, sea, and land based methods of transport. Navigation systems for each of these areas are also included in the Transportation market sector.

Aerospace – The Aerospace market sector is used to identify above atmosphere systems. This market sector includes space craft, satellites, and space stations. Ground stations that communicate with these systems are also included.

Military – The Military market sector describes entities that are involved with systems for military use. This includes weapons development, weapons control, and warning systems.

Consumer Electronics – The Consumer Electronics market sector includes the development and use of devices that are designed to be used around the home or by an individual. This market sector includes home automation systems, smart appliances, and mobile devices.

Facilities Infrastructure – The Facilities Infrastructure market sector encompasses the management of buildings and campuses. Facilities infrastructure includes corporate, residential, academic, and other types of facilities. This market sector includes building management and environmental controls such as heating and air conditioning.

Agriculture – The Agriculture market sector describes those entities that deal with the growth, processing, and distribution of food supplies. Uses of CPSs in this market sector include farm equipment, irrigation systems, food processing, and other applications.

Physical Access Control – The Physical Access Control market sector deals with the industries that are sometimes referred to as security. The term physical access control is designed to specify that the market sector focuses on physical security systems rather than cyber security systems.

Communications – The Communications market sector describes those victims concerned with voice, data, and video communications along with other communication mediums.

Construction – The Construction market sector is involved with the design and building of large projects. These could include buildings, roads, pipelines, and other types of facilities.

Entertainment Media Creation and Distribution – The Entertainment Media Creation and Distribution market sector is concerned with the production and distribution of media. This could include audio, video, and other forms of digital media. This market sector covers all of the different types of equipment and systems that would be used in this creation and distribution.

5.2.11 Summary

The classification of incidents by Source Type, Means, Impact, and Victim allows for practical analysis of incidents within a CPS. The sub-classification of Impact into Direct Impact, Indirect Impact, Severity of Impact, Immediacy of Impact, Recovery Time, and Monetary Impact makes it possible to conduct an impact oriented analysis of incidents. Classifying victims by their type along with their market sector allows for a cross domain analysis of incidents. This level of analysis, which is critical for CPS incidents, is not possible using any existing incident taxonomies. Figure 5-1 presents a tree based view of the final taxonomy.

5.3 Cyber-Physical Systems Incident Database

The Cyber-Physical Systems Incident Database (CPSID) is hosted in the Brigham Young University Cyber Security Research Lab. The server hosting the database has the following configuration:

Operating System: Debian 7 (linux 3.2.0-4-amd64)

Database Management System: SQLite 3.8.4.3

Web Front-End: Django 1.6.1

The database is currently hosted on a non-routable IP Address. After the database and web front-end have undergone a security evaluation, the web front-end will be made available at https://cpsid.csrl.et.byu.edu.

5.4 CPSID Workflow

Unfortunately, due to the malicious intent of a relative few, it is necessary to perform some sanitization of the public incident database to help minimize the risk of misuse. Two levels of protection are implemented in the online database. The first is the sanitization of records; this removes sensitive information and details from recorded incidents that may be misused. The second level of protection we shall implement is access control and a requirement to register for complete unsanitized access. Users will be required to register with a valid institutional, organizational, government, or recognized corporate domain. They will then be granted access subject to a basic verification of their request.

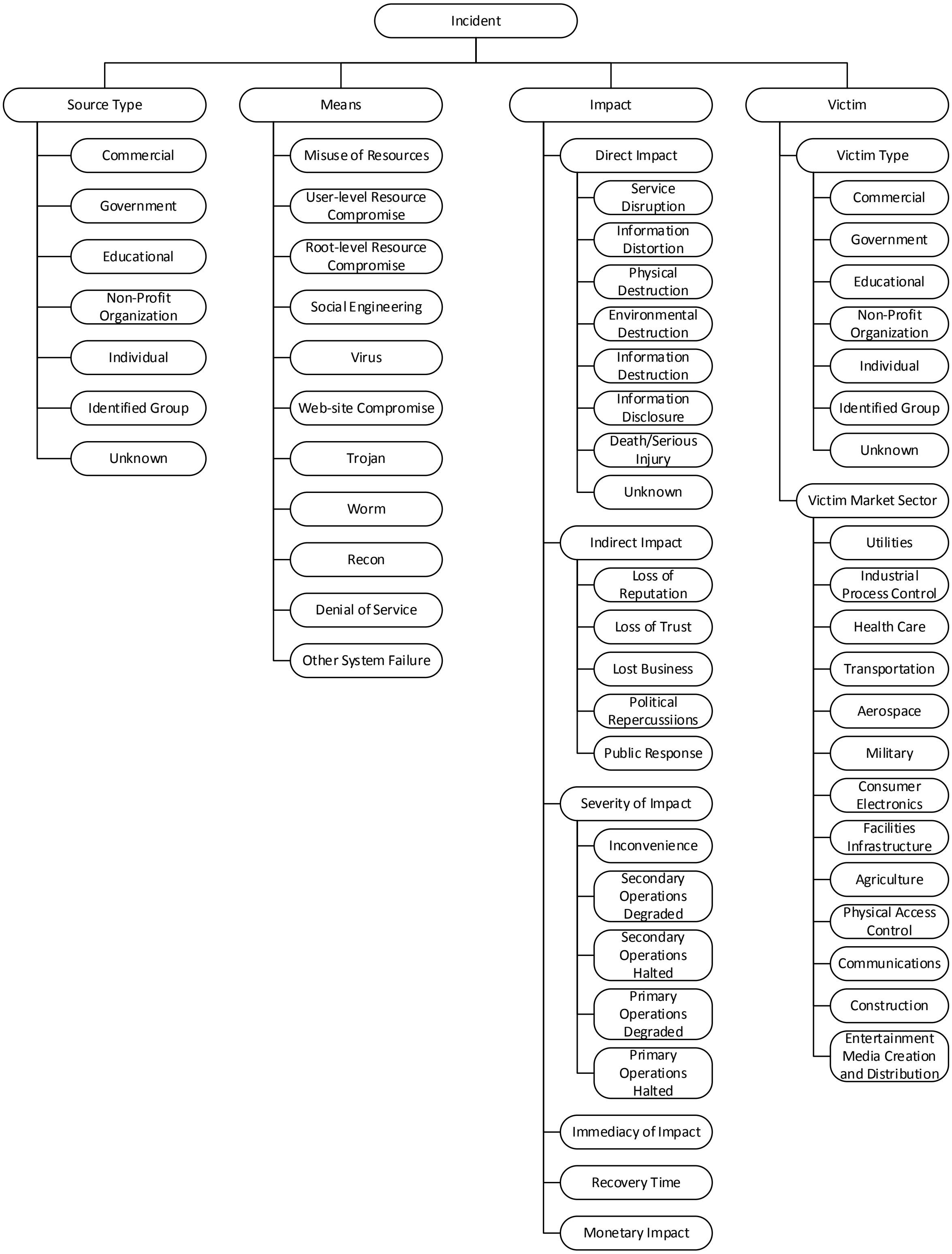


Figure 5-1: BYU-CPS Incident Taxonomy

5.4.1 User Registration Workflow

The user registration workflow is illustrated in Figure 5-2.

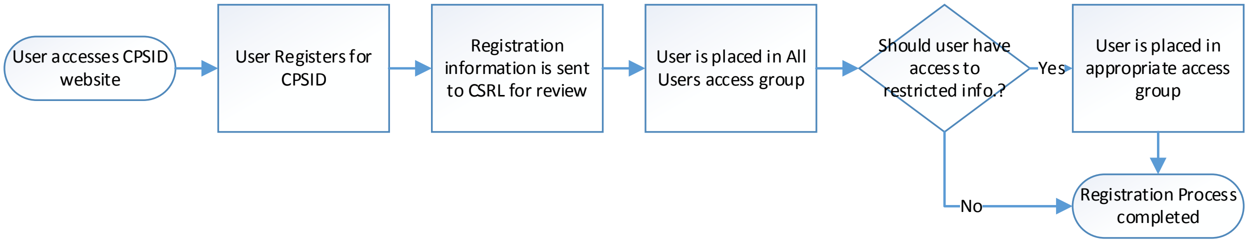

User accesses CPSID website
User Registers for CPSID
Registration information is sent to CSRL for review
User is placed in All Users access group
Should user have access to restricted info.?
Yes
User is placed in appropriate access group
No
Registration Process completed

Figure 5-2: CPSID User Registration Workflow

When a new user accesses the CPSID website, they will be prompted to register. By default, the user is placed in the All Users access group. Each registration request will be reviewed by a member of the CSRL to determine if further access is warranted. The available access groups are All Users, Authorized Users, Partners, Reviewers, and CSRL Admins. The Authorized Users group is for those who have a need to access sensitive information that is not available to the general public. The Partners group is for registered partners of the CSRL. These partners also have access to some of the sensitive information contained in the database. The Reviewers group is for authorized incident reviewers. Members of this group are responsible for reviewing the information in an incident report and determining the classification of the incident along with what information should be generally available and what should be restricted. The CSRL Admins group is for the CSRL administrators who are responsible for maintaining the system and assigning new incident reports to specific reviewers.

5.4.2 Incident Workflow

The user registration workflow is designed to make sure users have access to only the information appropriate for their level of access. There is a similar workflow for incident information to make sure the information is placed in the appropriate categories. The incident workflow is viewable in Figure 5-3.

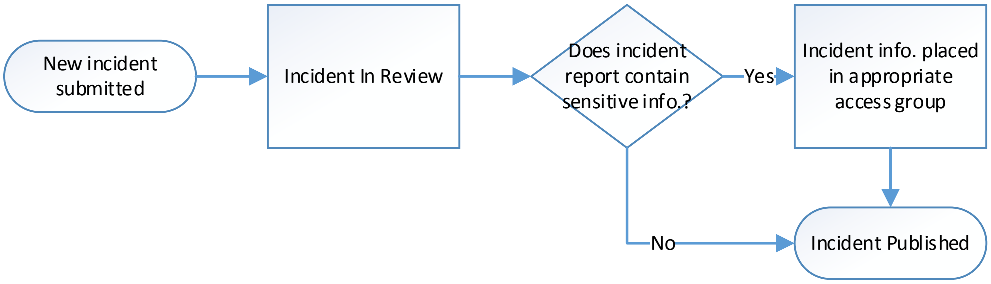

New incident submitted
Incident In Review
Does incident report contain sensitive info.?
Yes
Incident info. placed in appropriate access group
No
Incident Published

Figure 5-3: CPSID New Incident Workflow

When a new incident is submitted, it is only viewable by the submitter and the CSRL Admins group. A CSRL Admin will assign each incident to a specific reviewer. At that point, the incident is moved to the In Review status and is viewable by the assigned reviewer. The reviewer will then classify the incident according to the incident taxonomy and determine which information should be publicly available and which information is more sensitive. The sensitive information will then be flagged so that it is only available to the appropriate groups. This information could be flagged to be viewable by Authorized Users, Partners, or CSRL Members only. CSRL Members will have access to all information. Partners will have access to information in the Partners and Authorized Users groups. At this point, the incident is published according to the restrictions determined by the reviewer.

5.5 Framework Analysis and Observations

The proposed framework will provide a platform for studying CPS security incidents. This section will discuss how each component of the framework contributes to the overall ability to study these incidents.

5.5.1 BYU-CPS Incident Taxonomy

The taxonomy is the foundation for the proposed framework. The taxonomy is the component that provides the ability to compare and contrast incidents in multiple categories. The taxonomy can be useful in an overall comparison of CPS incidents; it is also useful for more detailed analysis within a specific category.

One of the goals of this research was to provide the ability to perform a cross-domain impact-oriented analysis of CPS incident. The proposed incident taxonomy provides the foundation for being able to perform this type of analysis. The classification categories as defined in the taxonomy have been selected and refined specifically for this purpose.

The initial plan was to use the database that has been developed to validate the taxonomy. This was to be accomplished by adding incidents to the database and determining whether the taxonomy categories as currently defined would describe each incident. Delays in the development of the database dictated the use of a manual validation process rather than utilizing the database.

The manual validation process proved to be of great benefit in the development of the taxonomy. The manual process allowed for more rapid updating of the taxonomy as changes could be made without the necessity of restructuring the database. Another benefit of the manual process was the ability to compare the classification of incidents within the new taxonomy to the classification of the same incidents using other available taxonomies.

The BYU-CPS Incident Taxonomy was validated by classifying the incidents as described in Chapter 3. These incidents were classified utilizing the Howard and Longstaff taxonomy, the Kjaerland taxonomy, and the AVOIDIT taxonomy. The results of these classifications were then compared with the classification according to the BYU-CPS Incident Taxonomy. The results of each classification are given here.

<u>Hospital Malware</u>

Howard and Longstaff Classification

Attackers – Vandals, *Tool* – Script or Program, *Vulnerability* – Configuration, *Action* – Modify, *Target* – Process, *Unauthorized Result* – Denial of Service, *Objectives* – Damage.

Kjaerland Classification

Source Sector – Unknown, *Method of Operation* – Virus, *Impact* – Disrupt, *Target Sector* – Com.

AVOIDIT Classification

Attack Vector – Misconfiguration/Kernel Flaws, *Operational Impact* – Installed Malware-Virus, *Defense – Mitigation* – Remove from Network, *Remediation* – Correct Code, *Informational Impact* – Disrupt, *Target* – OS.

BYU-CPS Incident Taxonomy Classification

Source Type – Unknown, *Means* – Virus, *Direct Impact* – Service Disruption, *Indirect Impact* – Loss of Trust, *Severity of Impact* – Primary Operations Degraded, *Immediacy of Impact* – Unknown, *Recovery Time* – Unknown, *Monetary Impact* – Unknown, *Victim Type* – Commercial, *Victim Market Sector* – Health Care.

Airport Hack

Howard and Longstaff Classification

Attackers – Hackers, *Tool* – Script or Program, *Vulnerability* – Design, *Action* – Modify, *Target* – Computer, *Unauthorized Result* – Denial of Service, *Objectives* – Challenge, Status, Thrill.

Kjaerland Classification

Source Sector – User, *Method of Operation* – Root Compromise/Denial of Service, *Impact* – Disrupt, *Target* – Gov.

AVOIDIT Classification

Attack Vector – Kernel Flaws, *Operational Impact* – Root Compromise, *Defense – Mitigation* – Remove from Network, *Remediation* – Correct Code, *Informational Impact* – Disrupt, *Target* – OS.

BYU-CPS Incident Taxonomy Classification

Source Type – Individual, *Means* – Root-level Resource Compromise, *Direct Impact* – Service Disruption, *Indirect Impact* – Loss of Trust, *Severity of Impact* – Secondary Operations Halted/Primary Operations Degraded, *Immediacy of Impact* – Unknown, *Recovery Time* – Six hours, *Monetary Impact* – Unknown, *Victim Type* – Government, *Victim Market Sector* – Transportation/Communications.

Pipeline Explosion

Howard and Longstaff Classification

This incident cannot be classified by Howard and Longstaff’s taxonomy.

Kjaerland Classification

Source Sector – Com/User, *Method of Operation* – Misuse of Resources, *Impact* – Disrupt, *Target Sector* – Com.

AVOIDIT Classification

This incident cannot be classified by the AVOIDIT taxonomy.

BYU-CPS Incident Taxonomy Classification

Source Type – Commercial, *Means* – Misuse of Resources/Other System Failure, *Direct Impact* – Physical Destruction/Environmental Destruction/Death/Serious Injury, *Indirect Impact* – Loss of Reputation/Loss of Trust/Lost Business/Political Repercussions/Public Response, *Severity of Impact* – Primary Operations Halted, *Immediacy of Impact* – Immediate, *Recovery Time* – Years, *Monetary Impact* – $200 Million, *Victim Type* – Commercial/Individual, *Victim Market Sector* – Utilities/Industrial Process Control.

Maroochy Water System

Howard and Longstaff Classification

Attackers – Hacker, *Tool* – User Command, *Vulnerability* – Implementation, *Action* – Spoof, *Target* – Process, *Unauthorized Result* – Increased Access/Corruption of Information, *Objectives* – Damage.

Kjaerland Classification

Source Sector – User, *Method of Operation* – Misuse of Resources/User Compromise, *Impact* – Disrupt, *Target Sector* – Gov.

AVOIDIT Classification

Attack Vector – Incorrect Permission, *Operational Impact* – Misuse of Resources/User Compromise, *Defense – Mitigation* – Unknown, *Remediation* – Correct Code, *Informational Impact* – Disrupt, *Target* – Application.

BYU-CPS Incident Taxonomy Classification

Source Type – Individual, *Means* – Misuse of Resources/User-level Resource Compromise, *Direct Impact* – Service Disruption/Environmental Destruction, *Indirect Impact* – Loss of Reputation/Political Repercussions, *Severity of Impact* – Primary Operations Degraded, *Immediacy of Impact* – Months, *Recovery Time* – Months, *Monetary Impact* – $50,000, *Victim Type* – Government, *Victim Market Sector* – Utilities/Industrial Process Control.

<u>Train System Virus</u>

Howard and Longstaff Classification

Attackers – Vandals, *Tool* – Autonomous Agent, *Vulnerability* – Configuration, *Action* – Modify, *Target* – Process, *Unauthorized Result* – Corruption of Information, *Objectives* – Damage.

Kjaerland Classification

Source Sector – Unknown, *Method of Operation* – Virus, *Impact* – Disrupt, *Target Sector* – Com.

AVOIDIT Classification

Attack Vector – Kernel Flaws/Incorrect Permission, *Operational Impact* – Installed Malware-Virus-File Infector-Worm-Mass Mailing, *Defense – Mitigation* –

Remove from Network, *Remediation* – Patch System, *Informational Impact* – Distort/Disclosure, *Target* – User.

BYU-CPS Incident Taxonomy Classification

Source Type – Unknown, *Means* – Virus, *Direct Impact* – Service Disruption, *Indirect Impact* – Loss of Reputation, *Severity of Impact* – Primary Operations Degraded, *Immediacy of Impact* – Immediate, *Recovery Time* – 24 hours, *Monetary Impact* – Unknown, *Victim Type* – Commercial, *Victim Market Sector* – Transportation.

Nuclear Power Plant Worm

Howard and Longstaff Classification

Attackers – Hackers, *Tool* – Autonomous Agent, *Vulnerability* – Configuration, *Action* – Flood, *Target* – Network, *Unauthorized Result* – Denial of Service, *Objectives* – Challenge, Status, Thrill.

Kjaerland Classification

Source Sector – Unknown, *Method of Operation* – Worm, *Impact* – Disrupt, *Target Sector* – Com.

AVOIDIT Classification

Attack Vector – Buffer Overflow, *Operational Impact* – Denial of Service, *Defense – Mitigation* – Remove from Network, *Remediation* – Patch System, *Informational Impact* – Disrupt, *Target* – Application/Server/DB/MSSQL Server.

BYU-CPS Incident Taxonomy Classification

Source Type – Unknown, *Means* – Worm, *Direct Impact* – Service Disruption, *Indirect Impact* – Loss of Reputation/Political Repercussions, *Severity of Impact* – Secondary Operations Halted, *Immediacy of Impact* – 8 hours, *Recovery Time* – 6 hours, *Monetary Impact* – Unknown, *Victim Type* – Commercial, *Victim Market Sector* – Utilities/Industrial Process Control.

Stuxnet

Howard and Longstaff Classification

Attackers – Spies, *Tool* – Autonomous Agent, *Vulnerability* – Configuration, *Action* – Modify, *Target* – Process, *Unauthorized Result* – Corruption of Information, *Objective* – Political Gain/Damage.

Kjaerland Classification

Source Type – Intl, *Method of Operation* – Worm/Root Compromise/Trojan, *Impact* – Disrupt/Distort, *Target Sector* – Gov.

AVOIDIT Classification

Attack Vector – Misconfiguration, *Operational Impact* – Root Compromise/Installed Malware – Trojan/Worm, *Defense* – *Mitigation* – Unknown, *Remediation* – Unknown, *Informational Impact* – Distort/Disrupt, *Target* – Application.

BYU-CPS Incident Taxonomy Classification

Source Type – Government, *Means* – Root-level Resource Compromise/Trojan/Worm, *Direct Impact* – Service Disruption/Physical Destruction, *Indirect Impact* – Political Repercussions, *Severity of Impact* – Primary Operations Degraded, *Immediacy of Impact* – Unknown, *Recovery Time* – Unknown, *Monetary Impact* – Unknown, *Victim Type* – Government, *Victim Market Sector* – Utilities/Industrial Process Control/Military.

Cellular Network Vehicle Attack

Howard and Longstaff Classification

Attackers – Not Defined, *Tool* – User Command, *Vulnerability* – Design, *Action* – Spoof, *Target* – Component, *Unauthorized Result* – Disclosure of Information/Corruption of Information, *Objectives* – Challenge, Status, Thrill.

Kjaerland Classification

Source Sector – Edu, *Method of Operation* – Misuse of Resources/Denial of Service, *Impact* – Disrupt/Distort/Disclosure, *Target Sector* – Com.

AVOIDIT Classification

Attack Vector – Design Flaws/Insufficient Input Validation, *Operational Impact* – Misuse of Resources/Denial of Service, *Defense – Mitigation* – None, *Remediation* – None, *Informational Impact* – Distort/Disrupt/Disclosure, *Target* – Application.

BYU-CPS Incident Taxonomy Classification

Source Type – Educational, *Means* – Misuse of Resources/Denial of Service, *Direct Impact* – Service Disruption/Information Disclosure, *Indirect Impact* – Loss of Reputation/Loss of Trust, *Severity of Impact* – Secondary Operations Degraded/Primary Operations Degraded, *Immediacy of Impact* –Unknown, *Recovery Time* – Unknown, *Monetary Impact* – Unknown, *Victim Type* – Commercial, *Victim Market Sector* – Transportation.

Summary of Classifications

The classification of each of these incidents utilizing each of these taxonomies is summarized in the following tables. Table 5-1 provides a summary of classifications according to Howard and Longstaff’s taxonomy.

Table 5-1: Summary of Howard and Longstaff Classifications

Incident	Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hospital Malware	Vandals	Script or Program	Configuration	Modify	Process	Denial of Service	Damage
Airport Hack	Hackers	Script or Program	Design	Modify	Computer	Denial of Service	Challenge, Status, Thrill
Pipeline Explosion	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined
Maroochy Water System	Hackers	User Command	Implementation	Spoof	Process	Increased Access, Corruption of Information	Damage
Train System Virus	Vandals	Autonomous Agent	Configuration	Modify	Process	Corruption of Information	Damage
Nuclear Power Plant Worm	Hackers	Autonomous Agent	Configuration	Flood	Network	Denial of Service	Challenge, Status, Thrill
Stuxnet	Spies	Autonomous Agent	Configuration	Modify	Process	Corruption of Information	Political Gain, Damage
Cellular Network Vehicle Attack	Undefined	User Command	Design	Spoof	Component	Disclosure of Information, Corruption of Information	Challenge, Status, Thrill

Table 5-2 presents the summary of classifications according to Kjaerland's taxonomy.

Table 5-2: Summary of Kjaerland Classifications

Incident	Source Sector	Method of Operation	Impact	Target Sector
Hospital Malware	Unknown	Virus	Disrupt	Com
Airport Hack	User	Root Compromise, Denial of Service	Disrupt	Gov
Pipeline Explosion	Com, User	Misuse of Resources	Disrupt	Com
Maroochy Water System	User	Misuse of Resources, User Compromise	Disrupt	Gov
Train System Virus	Unknown	Virus	Disrupt	Com
Nuclear Power Plant Worm	Unknown	Worm	Disrupt	Com
Stuxnet	Intl	Worm, Root Compromise, Trojan	Disrupt, Distort	Gov
Cellular Network Vehicle Attack	Edu	Misuse of Resources, Denial of Service	Disrupt, Distort, Disclosure	Com

Table 5-3 shows the summary of classifications of incidents utilizing the AVOIDIT taxonomy.

Table 5-3: Summary of AVOIDIT Classifications

Incident	Attack Vector	Operational Impact	Mitigation	Remediation	Informational Impact	Target
Hospital Malware	Misconfiguration, Kernel Flaws	Installed Malware – Virus	Remove from Network	Correct Code	Disrupt	OS
Airport Hack	Kernel Flaws	Root Compromise	Remove from Network	Correct Code	Disrupt	OS
Pipeline Explosion	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined
Maroochy Water System	Incorrect Permission	Misuse of Resources, User Compromise	Unknown	Correct Code	Disrupt	Application
Train System Virus	Kernel Flaws, Incorrect Permission	Installed Malware – Virus	Remove from Network	Patch System	Distort, Disclosure	User
Nuclear Power Plant Worm	Buffer Overflow	Denial of Service	Remove from Network	Patch System	Disrupt	Application
Stuxnet	Misconfiguration	Root Compromise, Installed Malware – Trojan/Worm	Unknown	Unknown	Distort, Disrupt	Application
Cellular Network Vehicle Attack	Design Flaws, Insufficient Input Validation	Misuse of Resources, Denial of Service	None	None	Distort, Disrupt, Disclosure	Application

Table 5-4 gives a summary of classifications utilizing the newly developed BYU-CPS Incident Taxonomy.

This classification exercise shows the benefits of utilizing the proposed taxonomy in classifying CPS incidents. An impact oriented approach to classification makes it possible to identify the impacts of an incident on the physical environment of the system. This approach also provides an ability to identify the interactions between cyber systems, physical systems, environmental systems, and social systems.

The cross domain approach to classification provides the ability to identify the interconnectedness of systems. There is no system that is completely isolated from everything else. Systems developers and engineers often perceive of their system as a stand-alone system without consideration for how the system interacts with other systems. The cross domain approach illustrates the flaws in this type of view. All systems are connected with other systems and those interactions and their consequences should be considered in any system design.

Table 5-4: Summary of BYU-CPS Incident Taxonomy Classifications

Incident	Source Type	Means	Direct Impact	Indirect Impact	Severity of Impact	Victim Type	Victim Market Sector
Hospital Malware	Unknown	Virus	Service Disruption	Loss of Trust	Primary Operations Degraded	Commercial	Health Care
Airport Hack	Individual	Root-level Resource Compromise	Service Disruption	Loss of Trust	Secondary Operations Halted, Primary Operations Degraded	Government	Transportation, Communications
Pipeline Explosion	Commercial	Misuse of Resources, Other System Failure	Physical Destruction, Environmental Destruction, Death/Serious Injury	Loss of Reputation, Loss of Trust, Lost Business, Political Repercussions, Public Response	Primary Operations Halted	Commercial, Individual	Utilities, Industrial Process Control
Maroochy Water System	Individual	Misuse of Resources, User-level Resource Compromise	Service Disruption, Environmental Destruction	Loss of Reputation, Political Repercussions	Primary Operations Degraded	Government	Utilities, Industrial Process Control
Train System Virus	Unknown	Virus	Service Disruption	Loss of Reputation	Primary Operations Degraded	Commercial	Transportation
Nuclear Power Plant Worm	Unknown	Worm	Service Disruption	Loss of Reputation, Political Repercussions	Secondary Operations Halted	Commercial	Utilities, Industrial Process Control
Stuxnet	Government	Root-level Resource Compromise, Trojan, Worm	Service Disruption, Physical Destruction	Political Repercussions	Primary Operations Degraded	Government	Utilities, Industrial Process Control, Military
Cellular Network Vehicle Attack	Educational	Misuse of Resources, Denial of Service	Service Disruption, Information Disclosure	Loss of Reputation, Loss of Trust	Secondary Operations Degraded, Primary Operations Degraded	Commercial	Transportation

5.5.2 Cyber-Physical Systems Incident Database

An analysis of CPS incidents requires us to have information about each of these incidents. This is the role of the CPSID. The CPSID is designed to be a repository for all available information about known CPS incidents. An issue with this type of repository is the security of the information contained within the repository. There are some who would attempt to access the information within the repository for malicious purposes. The repository must be made secure to minimize the risk that sensitive information will be made available to the wrong people.

5.5.3 CPSID Workflow

The CPSID workflow is designed to aid with the security of the CPSID. The user registration workflow allows for users to be assigned to groups that provide access to the information they require while restricting access to more sensitive information. The incident workflow is designed to place information about each incident in the proper categories to allow information to be available only to those who have a need to access it. While it is acknowledged that no system is completely secure, the CPSID workflow is designed to make the information contained within the database as secure as possible while still making it available to those with a legitimate need for access.

5.6 Chapter Summary

The proposed framework has three components: the BYU-CPS Incident Taxonomy, the Cyber-Physical Systems Incident Database, and the CPSID Workflow. These components are designed to work together to consolidate information about CPS incidents and provide that information to those who need it. These components are also designed to make sensitive information about incidents secure and unavailable to those who would use the information maliciously.

The proposed taxonomy was validated through classifying several CPS incidents. These same incidents were classified using other available taxonomies to provide a comparison. This validation and comparison exercise identified the benefits of using the proposed taxonomy in classifying CPS incidents.

6 CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter will provide an analysis of each of the research questions and hypotheses presented in Chapter 1. A discussion of how each question and hypothesis was answered will be presented. Some recommendations and plans for future work will also be presented. Finally, this chapter will summarize what has been achieved through this research.

6.2 Conclusions

The research questions and hypothesis were presented in three general questions: Taxonomy Categories, Suitable Methods for Measuring the Impact of an Incident, and Identifiable Benefits. Each of these will be discussed in turn.

6.2.1 Taxonomy Categories

A new incident taxonomy that is focused on CPS incidents has been created. This taxonomy is designed to allow a cross domain, impact oriented analysis of incidents. The cross domain analysis provides insights into how systems interact with each other. This analysis is provided through the use of market sectors in the classification of incidents. The impact oriented approach identifies the effects an incident has not only on the system where the incident occurs but also on the surrounding environment.

The creation of a new taxonomy for classifying CPS incidents identified the categories that would allow for cross domain analysis of incidents. These categories are Victim Type and Victim Market Sector. The Victim Type category provides a description of the general characteristics of the victim of an incident. This description allows for analysis based on these types. The Victim Market Sector category provides detail for the sector in which a victim is involved. This detail demonstrates the cross domain nature of CPSs and the interconnectedness of these systems. The cross domain analysis of incidents shows that no system operates in isolation. Every system is connected to other systems whether cyber, physical, environmental, or social.

The new taxonomy also provides categories for an impact oriented analysis of incidents. The Direct Impact category defines the impacts an incident can have on the CPS and on the surrounding environment. This surrounding environment includes the entity that operates the CPS, the people who live around the CPS, and the natural environment. The Indirect Impact category provides a view into the long-term effects an incident has on the entity that operates the CPS. These long-term effects are often overlooked in the analysis of an incident. The modifiers of Immediacy of Impact, Recovery Time, and Monetary Impact also provide insight into effects of an incident that many times go unnoticed.

Chapters 3, 4, and 5 answer Q1 “What taxonomy categories will allow for cross domain analysis of incidents?” as Victim Type and Victim Market Sector. The victim type allows for analysis according to general characteristics of the victim. The victim market sector allows for analysis based on the domain of a victim and how that domain may be perceived by different people.

Chapters 3, 4, and 5 answer Q2 “What taxonomy categories will allow for an impact oriented analysis of incidents?” as Direct Impact and Indirect Impact with modifiers for Immediacy of Impact, Recovery Time, and Monetary Impact. The direct impact category provides information about the immediate effects of an incident. The indirect impact category provides insight into the long-term consequences of an incident. The modifiers provide methods for comparing these immediate and long-term effects across incidents.

6.2.2 Suitable Methods for Measuring the Impact of an Incident

The ability to measure the impact of an incident is always difficult. Most measures rely on some form of Low/Medium/High scale of severity. The newly created taxonomy modifies this scale to make it more appropriate for CPSs. The modified scale classifies the severity of an impact as Inconvenience, Secondary Operations Degraded, Secondary Operations Halted, Primary Operations Degraded, and Primary Operations Halted. This scale provides a general low severity (Inconvenience). The medium and high severities are divided between primary and secondary operations.

Chapters 3, 4, and 5 answer H1 “Suitable methods for measuring the impact of an incident currently exist.” as true. A Low/Medium/High scale is generally suitable for measuring the impact of an incident.

Chapters 3, 4, and 5 answer H2 “Currently available methods can be adapted for use in CPS incidents.” as true. The Low/Medium/ High scale can be modified as Inconvenience, Secondary Operations Degraded, Secondary Operations Halted, Primary Operations Degraded, and Primary Operations Halted to account for the unique nature of CPS incidents.

6.2.3 Identifiable Benefits

The benefits of doing cross domain, impacted oriented analysis of incidents were identified by classifying a representative sample of incidents utilizing different taxonomies. The results of this classification exercise were compared to the newly created taxonomy to provide an analysis of benefits of the new classification system.

A cross domain classification system provides the ability to understand how a system does not reside in a single domain. Most systems are designed with a single domain in mind, but these domains are interconnected in ways that are often not understood or overlooked. It is impossible to isolate a system to a single domain. Cross domain analysis shows us not only how systems are connected to and interact with each other, but also how a system that may be perceived to be in one domain could also be perceived to be in another domain depending on one's point of view.

An impact oriented approach to classifying incidents provides insight into the effects an incident has on the system and surrounding environment. In a CPS, the surrounding environment includes the physical aspects of the system, the natural environment the system is located in, and the social environment of the community where the system resides. An incident within a CPS impacts all of these environments. An impact oriented approach also provides means for analyzing the long term effects of an incident on the entity that operates the CPS. These long term effects may drastically change the way the entity operates in the future.

Chapters 3, 4, and 5 answer Q3 "What are the identifiable benefits of a cross domain classification system?" as: Cross domain analysis provides insights into the interconnectedness of CPSs and that systems may be perceived to be in different domains based on the point of view of the observer.

Chapters 3, 4, and 5 answer Q4 “What are the identifiable benefits of an impact oriented classification system?” as: An impact oriented approach to classification provides insight into the immediate and long-term effects of an incident on the entity where the incident occurs and the surrounding environment.

6.3 Recommendations

This research has provided a taxonomy that is suitable for classifying incidents within a CPS. A database to catalog these incidents based on the new taxonomy has also been created. This database has been designed to be a publicly available repository of information about CPS incidents that is freely available for academic research. A beginning set of incidents has been classified and added to this database. The maintenance of this database should be an ongoing effort of the Brigham Young University Cyber Security Research Lab.

This research has been focused on the development of the incident taxonomy and repository. No attempt has been made to analyze the contents of the database. A methodology for analyzing the contents of the database needs to be developed. This analysis should focus on identifying trends, commonalities, and differences in these incidents. This analysis should provide understanding into how CPS incidents happen and how they can be prevented.

Understanding that it is impossible to prevent all possible incidents, steps need to be taken to minimize the occurrence of incidents and the impact these incidents have. The analysis of incidents included in this database should be used to develop these methodologies for minimizing both the occurrence and impact of CPS incidents. Above all, these methodologies should focus on protecting the people and the environment that surround these systems.

6.3.1 Future Work

The initial goal of this work was to complete the CPSID and make it publicly available. Development delays have made this goal unattainable at this time. The database has been developed and is currently being populated with incidents. The web front end still needs to be developed and undergo a comprehensive security evaluation. After the evaluation, the front end will be modified to correct any issues that are discovered. The web front end will then be made available. Once available, the CPSID will need to be marketed to encourage adoption within the academic and research communities. Efforts will also need to be made to encourage industry participation in the CPSID.

The proposed framework provides a foundation for studying CPS incidents. The framework as proposed will require ongoing maintenance. As new incidents are discovered, they will need to be added to the database. New incidents may have characteristics that require the BYU-CPS Incident Taxonomy to be updated to maintain relevance. Incidents already cataloged in the database will need to be updated as new information becomes available. Ongoing review of those who have access to the CPSID will also be required to maintain security. There will also be a need to maintain the infrastructure supporting the CPSID (Hardware, Operating Systems, Applications, etc.) to ensure continued support and security.

This framework could be extended to provide statistical analysis of incidents contained in the CPSID. This analysis could then be used to develop best practices for security within a CPS. These best practices should include both design and implementation considerations for a CPS. The best practices should then be adopted by industry as they build new CPSs and improve existing ones.

The overall goal of this research is to make the use of CPSs more safe and secure. The achievement of this goal will require a collaborative effort between academic researchers and industry. The CPSID should be used as an instrument to facilitate this collaboration. The collaborative efforts of academia and industry will provide the knowledge of security flaws within CPSs along with the expertise to fix those flaws and create a safer and more secure product for the end users and the surrounding communities.

6.4 Achievements of this Research

This research began as an attempt to document several cyber-security incidents involving SCADA and Critical Infrastructure. This attempt led to the discovery that currently available incident taxonomies were insufficient for analyzing incidents involving a CPS. The first achievement of this research is the production of a new taxonomy that is focused solely on CPS incidents. This new taxonomy provides several benefits over currently existing taxonomies when it comes to classifying incidents that involve a CPS:

- The newly developed taxonomy provides the ability to analyze the impacts of an incident with a unique view to CPSs. A CPS incident involves the physical world along with the cyber-component. This taxonomy provides methods for analyzing these physical impacts along with the cyber impacts that currently available taxonomies address.
- The newly developed taxonomy provides the ability to perform a cross-domain analysis of incidents. The inclusion of market sectors in the taxonomy allows for a researcher to see how a single incident may impact multiple domains. It also provides the ability to see if similar incidents have different impacts based on the domain of the system in which the incident occurs.

This research has also developed the CPSID. The CPSID is a repository for information about incidents involving CPSs. The benefits of the CPSID as defined in this research are:

- The CPSID provides information on incidents in all areas of CPS. It is not focused solely on Critical Infrastructure or SCADA systems as the currently available databases are.
- The CPSID is freely available for academic research. This overcomes the barrier of having to pay thousands of US dollars per year for access to information about these incidents.

In conclusion, this research has provided a solution to the problem as stated in Chapter 1. This research has produced a cross-domain impact-oriented classification system and database that are freely available for academic research into CPS incidents.

REFERENCES

Blackwell, Clive. 2010. “A Security Ontology for Incident Analysis.” In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW ’10*, 1. New York, New York, USA: ACM Press. doi:10.1145/1852666.1852717. http://dl.acm.org/citation.cfm?id=1852666.1852717.

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” In *Proceedings of the 20th USENIX Conference on Security*, 6. Berkeley, CA, USA: USENIX Association. http://dl.acm.org/citation.cfm?id=2028067.2028073.

“CVE - Common Vulnerabilities and Exposures (CVE).” http://cve.mitre.org/.

Denning, Dorothy E. 2000. “Cyberterrorism: The Logic Bomb versus the Truck Bomb - Centre for World Dialogue.” *Global Dialogue* 2 (4). http://www.worlddialogue.org/content.php?id=111.

Farwell, James P., and Rafal Rohozinski. 2011. “Stuxnet and the Future of Cyber War.” *Survival* 53 (1) (February): 23–40. doi:10.1080/00396338.2011.555586.

Hansman, Simon, and Ray Hunt. 2005. “A Taxonomy of Network and Computer Attacks.” *Computers & Security* 24 (1): 31–43. http://www.sciencedirect.com/science/article/pii/S0167404804001804.

Helps, Richard, and Francis Mensah. 2012. “Comprehensive Design of Cyber Physical Systems.” In *Proceedings of the 13th Annual Conference on Information Technology Education (SIGITE ’12)*, 233–238. New York, New York, USA: ACM. http://sigite2012.sigite.org/wp-content/uploads/2012/08/session16-paper03.pdf.

Howard, John D., and Thomas A. Longstaff. 1998. “A Common Language for Computer Security Incidents.” *Sandia Report: SAND98-8667, ...* (October). http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf.

Kjaerland, Maria. 2006. “A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors.” *Computers & Security* 25 (7) (October): 522–538. doi:10.1016/j.cose.2006.08.004. http://dx.doi.org/10.1016/j.cose.2006.08.004.

Miller, Bill, and Dale Rowe. 2012. "A Survey of SCADA and Critical Infrastructure Incidents." In *Proceedings of the 1st Annual Conference on Research in Information Technology - RIIT '12*, 51–56. New York, New York, USA: ACM Press. doi:10.1145/2380790.2380805. http://dl.acm.org/citation.cfm?doid=2380790.2380805.

Mirkovic, Jelena, and Peter Reiher. 2004. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms." *ACM SIGCOMM Computer Communication Review* 34 (2) (April 1): 39. doi:10.1145/997150.997156. http://dl.acm.org/citation.cfm?id=997150.997156.

Mustard, Steve. 2005. "Security of Distributed Control Systems: The Concern Increases." *Computing & Control Engineering Journal*. doi:10.1049/ccej:20050605.

Nicholson, Andrew, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. 2012. "SCADA Security in the Light of Cyber-Warfare." *Computers & Security* 31 (4) (March): 436–418. doi:10.1016/j.cose.2012.02.009. http://dx.doi.org/10.1016/j.cose.2012.02.009.

OWASP. "OWASP Risk Rating Methodology." https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

Ozdemir, Engin, and Mevlut Karacor. 2006. "Mobile Phone Based SCADA for Industrial Automation." *ISA Transactions* 45 (1) (January): 67–75. doi:10.1016/S0019-0578(07)60066-4. http://www.sciencedirect.com/science/article/pii/S0019057807600664.

Poovendran, Radha. 2010. "Cyber–Physical Systems: Close Encounters Between Two Parallel Worlds [Point of View]." *Proceedings of the IEEE* 98 (8) (August): 1363–1366. doi:10.1109/JPROC.2010.2050377. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5512708.

Poulsen, Kevin. 2003. "Slammer Worm Crashed Ohio Nuke Plant Network." *Security Focus*, August. http://www.securityfocus.com/news/6767.

Rajkumar, Ragunathan (Raj), Insup Lee, Lui Sha, and John Stankovic. 2010. "Cyber-Physical Systems." In *Proceedings of the 47th Design Automation Conference on - DAC '10*, 731. New York, New York, USA: ACM Press. doi:10.1145/1837274.1837461. http://dl.acm.org/citation.cfm?id=1837274.1837461.

RISI. 2014. "RISI - The Repository of Industrial Security Incidents." Accessed May 2. http://securityincidents.org/.

Simmons, Chris, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. 2009. "AVOIDIT: A Cyber Attack Taxonomy." *University of Memphis, Technical Report CS-09-003*. http://si.lopesgazzani.com.br/docentes/marcio/SegApp/CyberAttackTaxonomy_IEEE_Mag.pdf.

Sveen, Finn Olav, Jose M Sarriegi, Eliot Rich, and Jose J Gonzalez. 2007. “Toward Viable Information Security Reporting Systems.” *Information Management & Computer Security* 15 (5): 408–419. http://search.proquest.com/docview/212305977?accountid=4488.

Talbot, David. 2012. “Computer Viruses Are ‘Rampant’ on Medical Devices in Hospitals.” *Technology Review*. http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices/.

Tsang, Rose. 2012. “Cyberthreats, Vulnerabilities and Attacks on SCADA Networks.” Accessed June 5. http://gspp.berkeley.edu/iths/Tsang_SCADA Attacks.pdf.

US-CERT. 2014. “US-CERT | United States Computer Emergency Readiness Team.” Accessed January 5. http://www.us-cert.gov/.

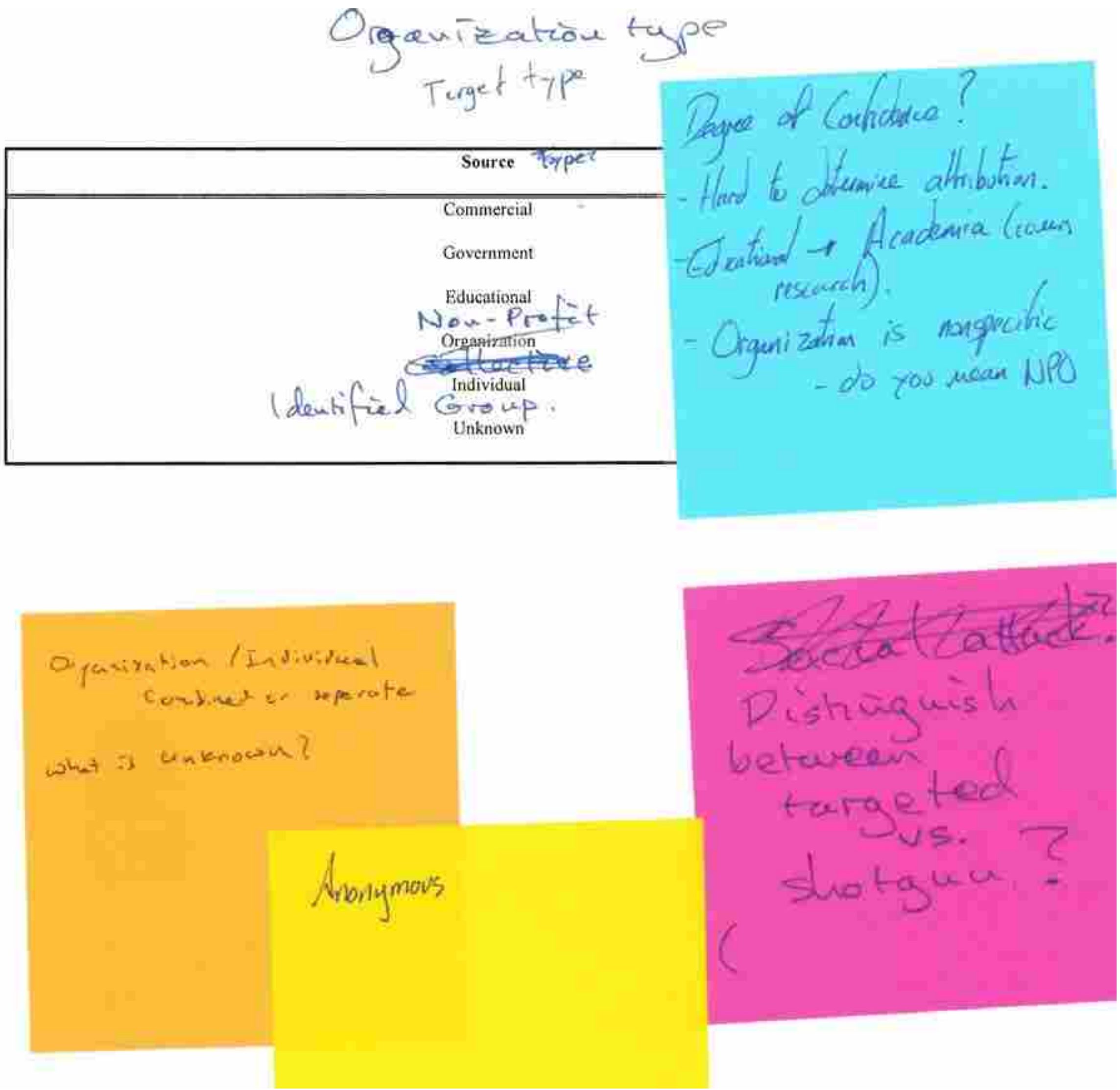
Weaver, Nicholas, Vern Paxson, Stuart Staniford, and Robert Cunningham. 2003. “A Taxonomy of Computer Worms.” In *Proceedings of the 2003 ACM Workshop on Rapid Malcode - WORM’03*, 11. New York, New York, USA: ACM Press. doi:10.1145/948187.948190. http://dl.acm.org/citation.cfm?id=948187.948190.

Zhu, Bonnie, Anthony Joseph, and Shankar Sastry. 2011. “A Taxonomy of Cyber Attacks on SCADA Systems.” In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. IEEE. doi:10.1109/iThings/CPSCom.2011.34. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6142258.

APPENDICES

APPENDIX A. AFFINITY DIAGRAM TECHNIQUE FOR TAXONOMY REFINEMENT

After the initial taxonomy was created, the results were brought before the research group for further refinement. This refinement utilized an affinity diagram technique where each member of the group wrote comments about the different categories within the taxonomy. These notes were then discussed to determine the changes that were needed. The notes from this exercise may be seen in the following figures.



Organization type
Target type

Source Type?
Commercial
Government
Educational
Non-Profit Organization
~~Collective~~
Individual
Identified Group.
Unknown

Degree of Confidence?
- Hard to determine attribution.
- Educational → Academia (cover research).
- Organization is nonspecific
  - do you mean NPO

Organization / Individual
combined or seperate

what is unknown?

Anonymous

~~Social attack?~~
Distinguish
between
targeted
vs. ?
shotgun?
(

Means
Misuse of Resources
User Compromise
Root Compromise
Social Engineering
Virus
Web Compromise
Trojan
Worm
Recon
Denial of Service
Other Sys Failure

- Data interception
- compromised partner
-

Put in verb-subject form

e.g. "compromise user"

Is Means correct title?

Means → Cause?

Groupings:

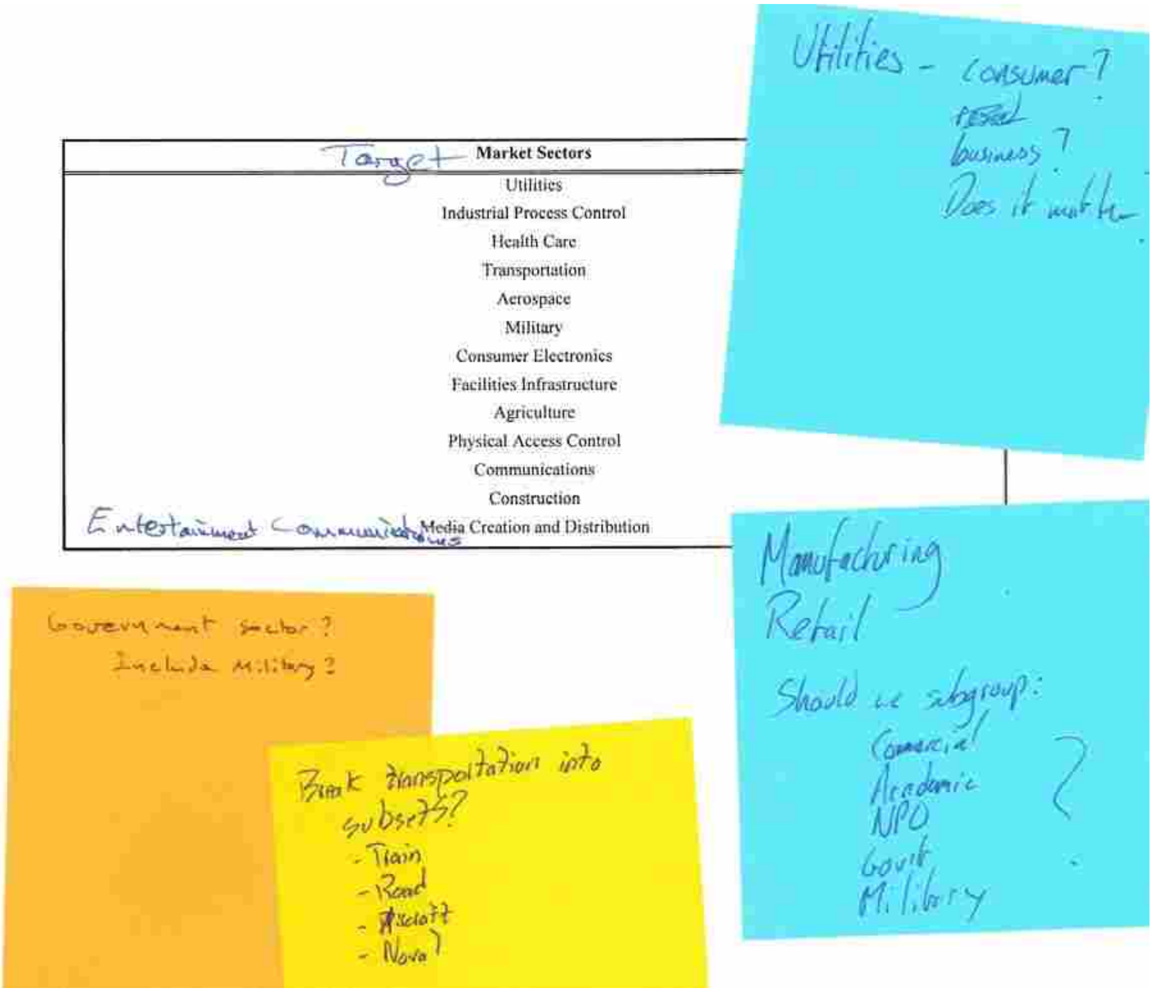
Human (direct)

Malware {

Failure

Disaster

Other Incident



Target Market Sectors
Utilities
Industrial Process Control
Health Care
Transportation
Aerospace
Military
Consumer Electronics
Facilities Infrastructure
Agriculture
Physical Access Control
Communications
Construction
Entertainment Communications Media Creation and Distribution

Utilities - consumer?
resell
business?
Does it matter

Manufacturing
Retail

Should we subgroup:
Commercial
Academic
NPO
Gov't
Military
?

Government sector?
Include Military?

Break transportation into subsets?
- Train
- Road
- Aircraft
- Naval

- Maybe D's is using letter rather than Clarity?
- Is each term information system or service centric?

Impact
Disrupt
Distort
Destroy
Disclose
Death/Serious Injury
Unknown

~~Intangible~~ Check-box
Indirect (Reputation, loss of trust)
~~etc~~, Lost Business
Political repercussions
Public Response

Removed / Stolen?
Combination of impact?
Degree of impact?
ie: disclosure to whom?
single entity?
general public?

Scale in
$$ and/or
in "time-to-repair"
and/or
~~downtime~~ ?
tolor
time

Where is
"immediacy of problem"?
>Traffic disruption
minutes
>Water supply
days
>Elec failure
-> seconds

Difference btwn
"criticality
&
Impact?"

Modifier of Impact

~~Criticality~~ (Severity)
Inconvenience
Secondary Operations Affected
Primary Operations Affected
Primary Operations Halted
~~Human Life Affected~~

Human Life
Death / Injury
Different Levels?

Impact vs Criticality
should probably
be mutually exclusive
Criticality a modifier on
impact?

Tolerance

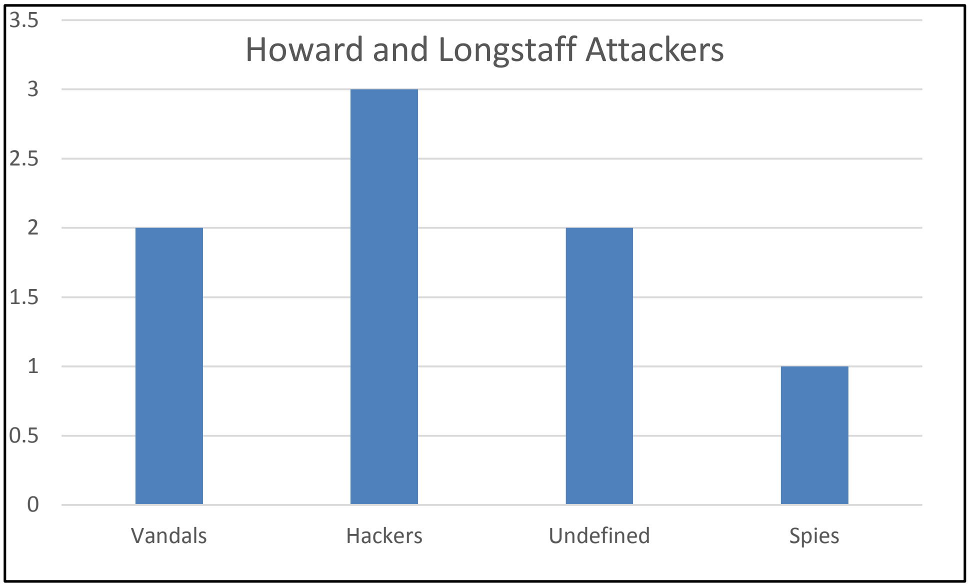
Immediacy Modifier of Impact

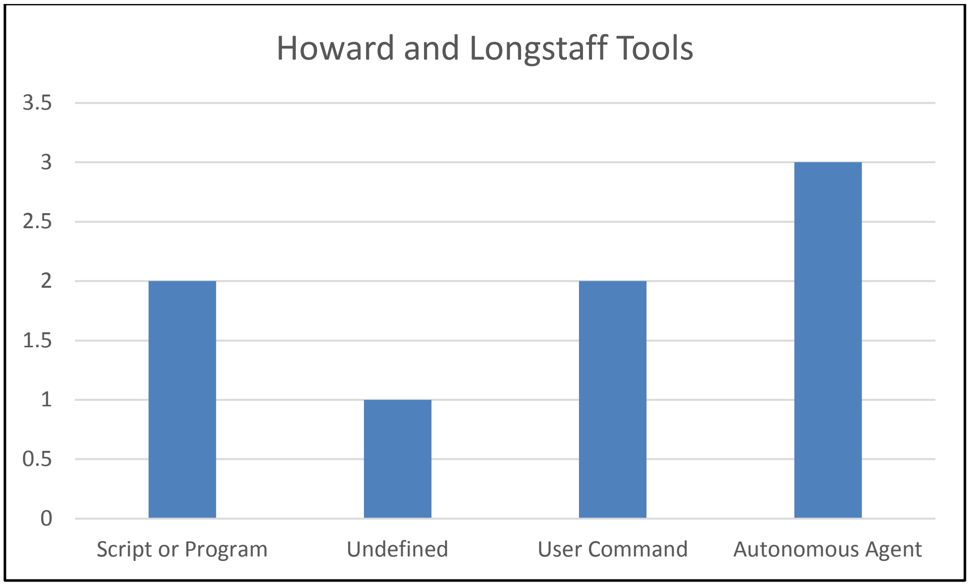
seconds
minute
hours
days
Longer

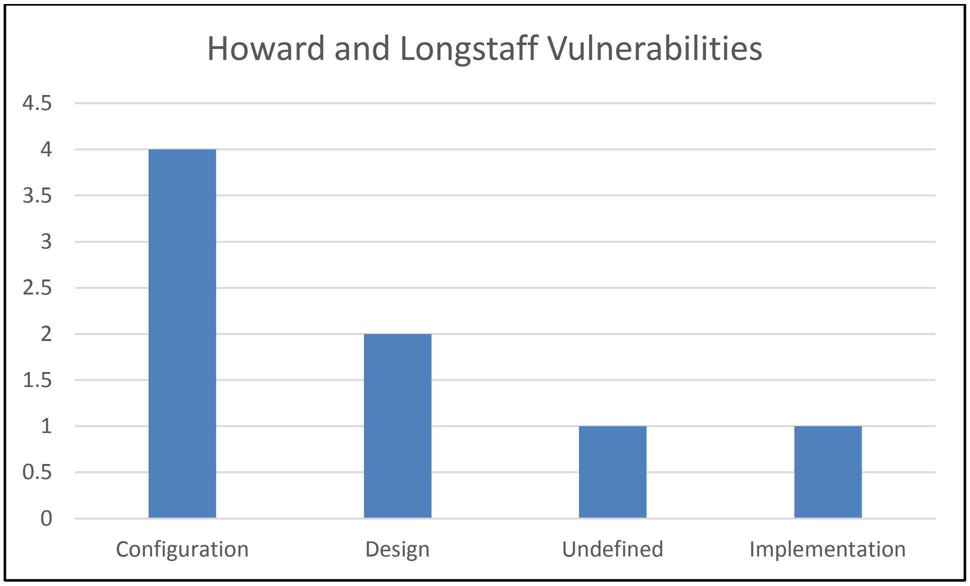
Recovery Time

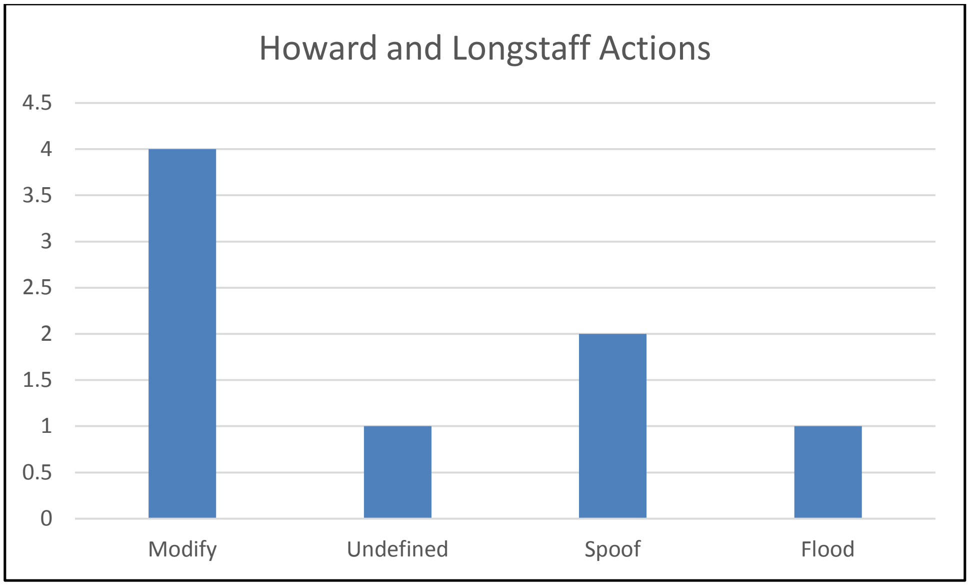
APPENDIX B. SUMMARY OF CLASSIFICATION DISTRIBUTIONS

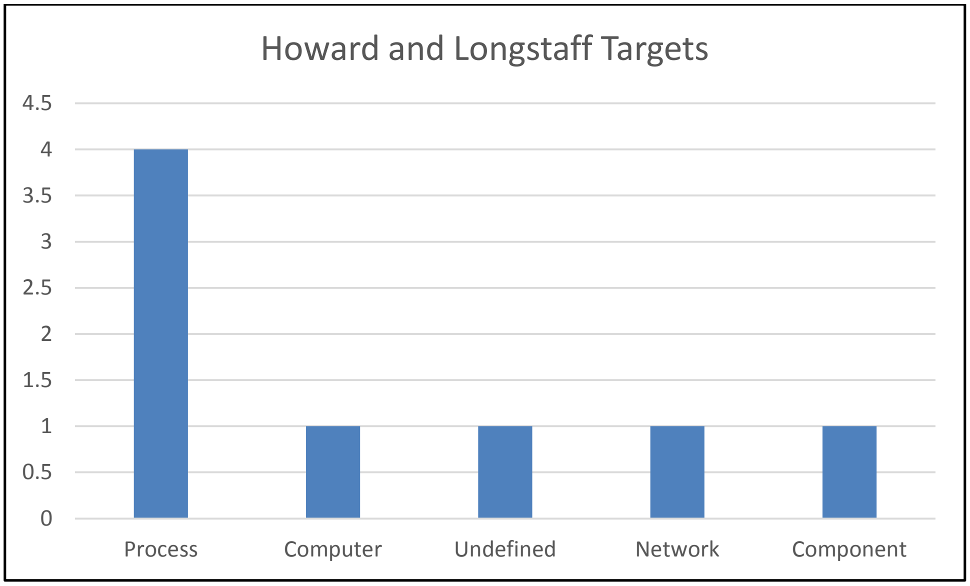
The following figures represent the distribution of classifications according to the Howard and Longstaff taxonomy.

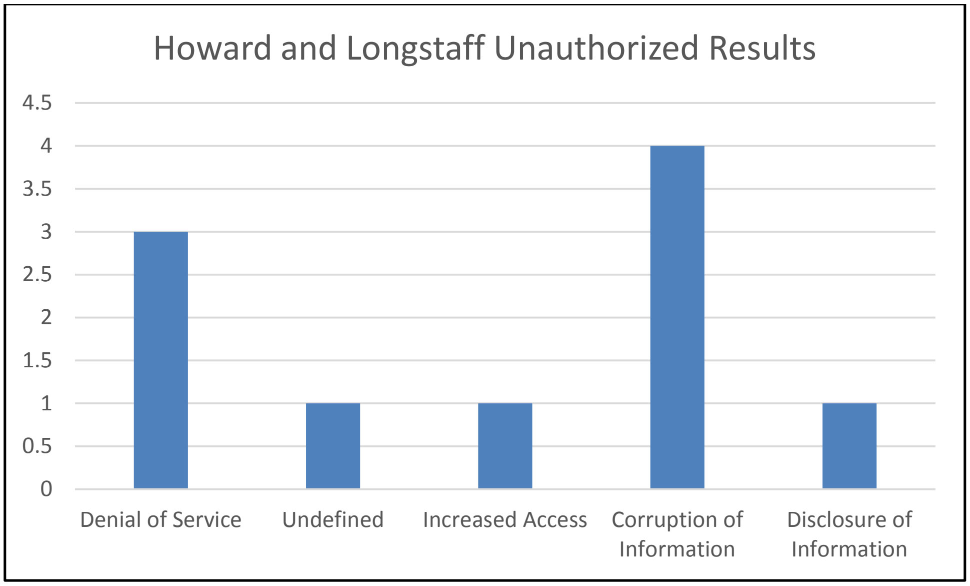


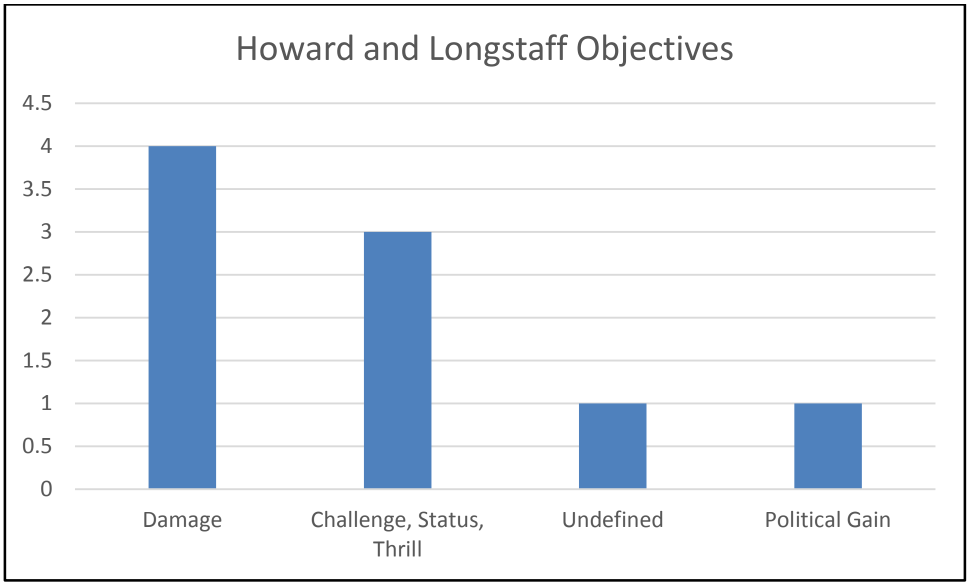

Howard and Longstaff Tools
3.5
3
2.5
2
1.5
1
0.5
0
Script or Program
Undefined
User Command
Autonomous Agent


Howard and Longstaff Vulnerabilities
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Configuration
Design
Undefined
Implementation

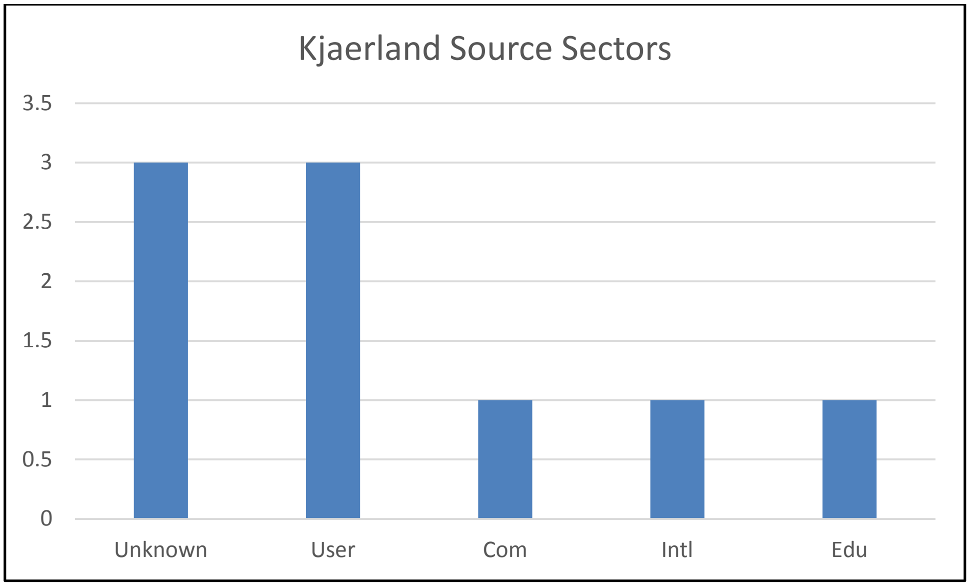

Howard and Longstaff Actions
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Modify
Undefined
Spoof
Flood

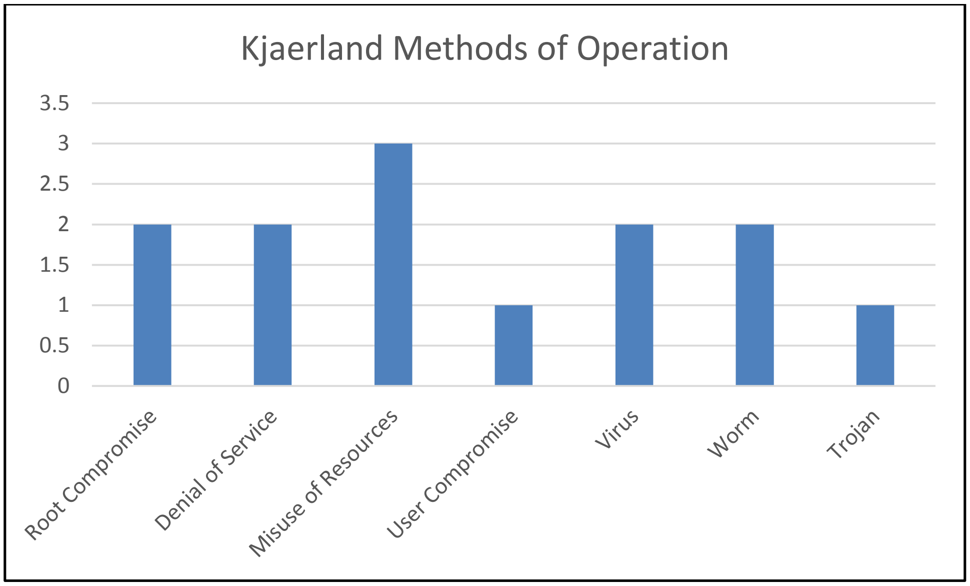

Howard and Longstaff Targets
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Process
Computer
Undefined
Network
Component

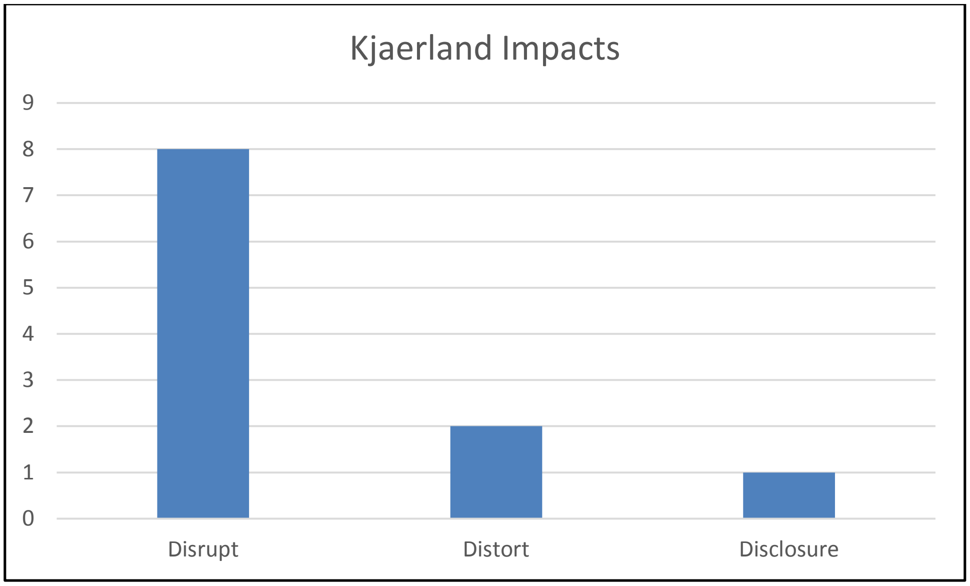

Howard and Longstaff Unauthorized Results
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Denial of Service
Undefined
Increased Access
Corruption of Information
Disclosure of Information

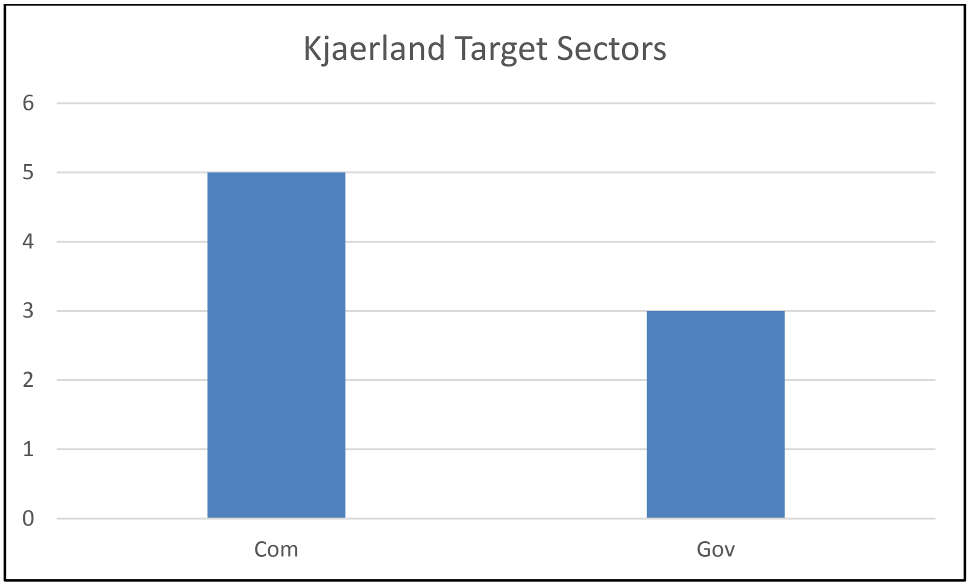

Howard and Longstaff Objectives
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Damage
Challenge, Status, Thrill
Undefined
Political Gain

The following graphs present the distribution of classifications according to Kjaerland's taxonomy.

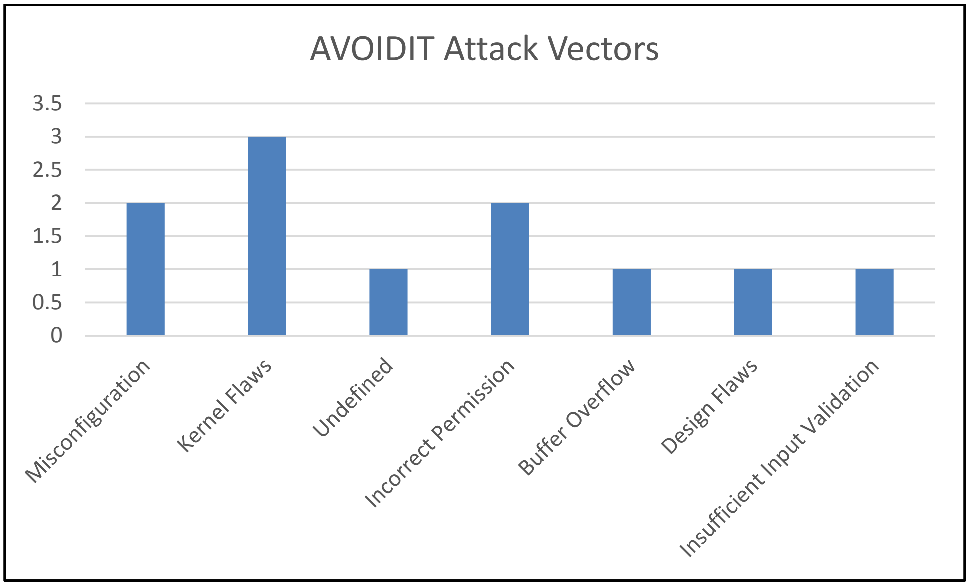


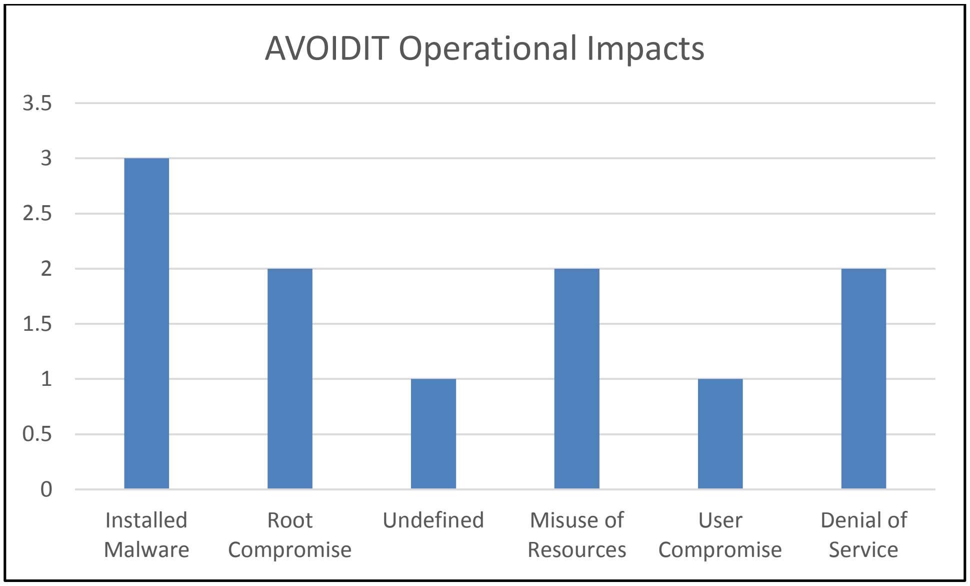


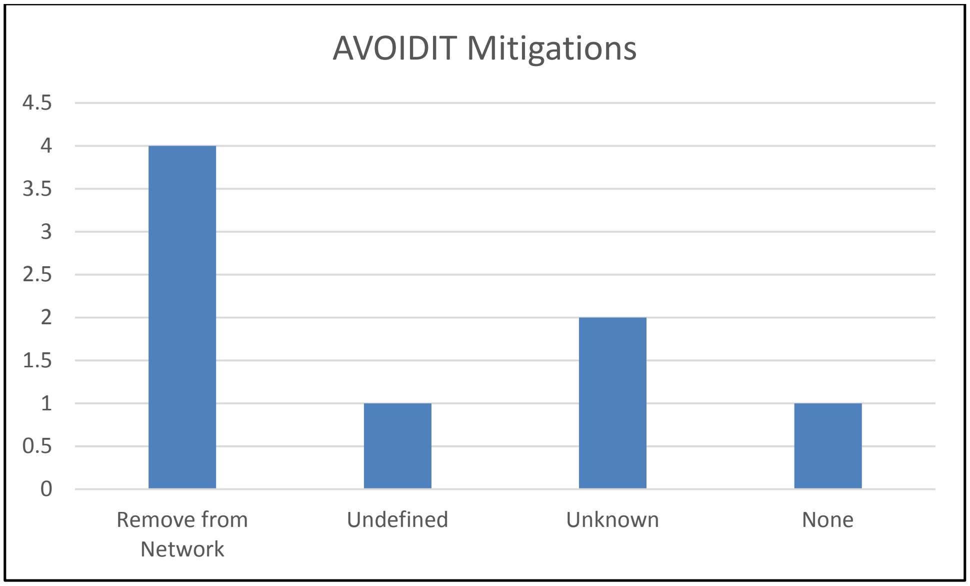

Kjaerland Impacts
9
8
7
6
5
4
3
2
1
0
Disrupt
Distort
Disclosure

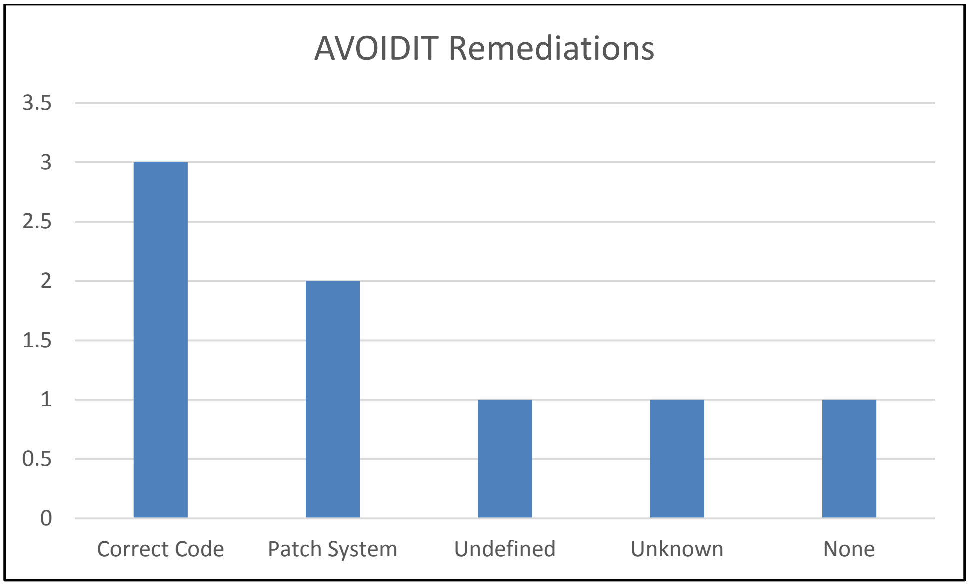

Kjaerland Target Sectors
6
5
4
3
2
1
0
Com
Gov

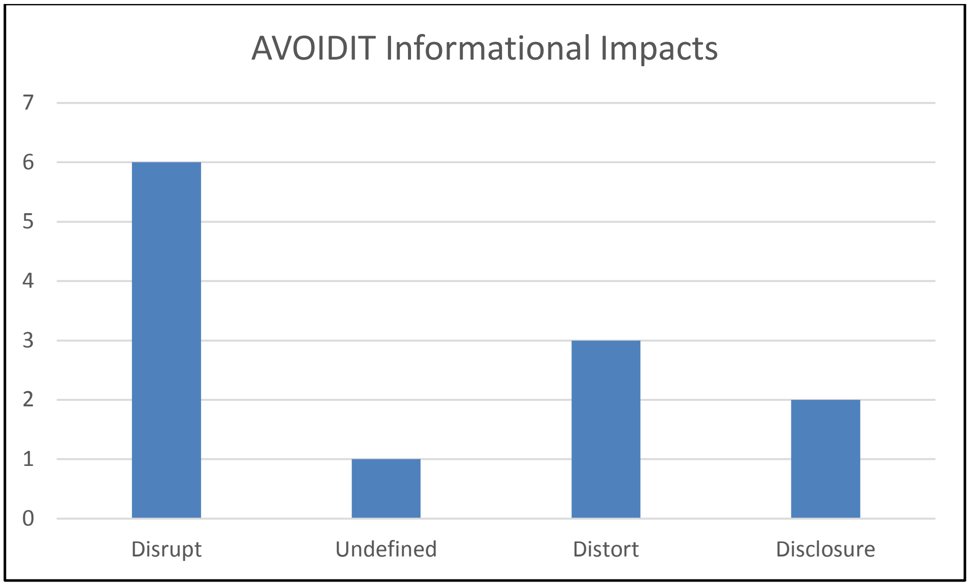
The following charts display the distribution of classifications when utilizing the AVOIDIT taxonomy.

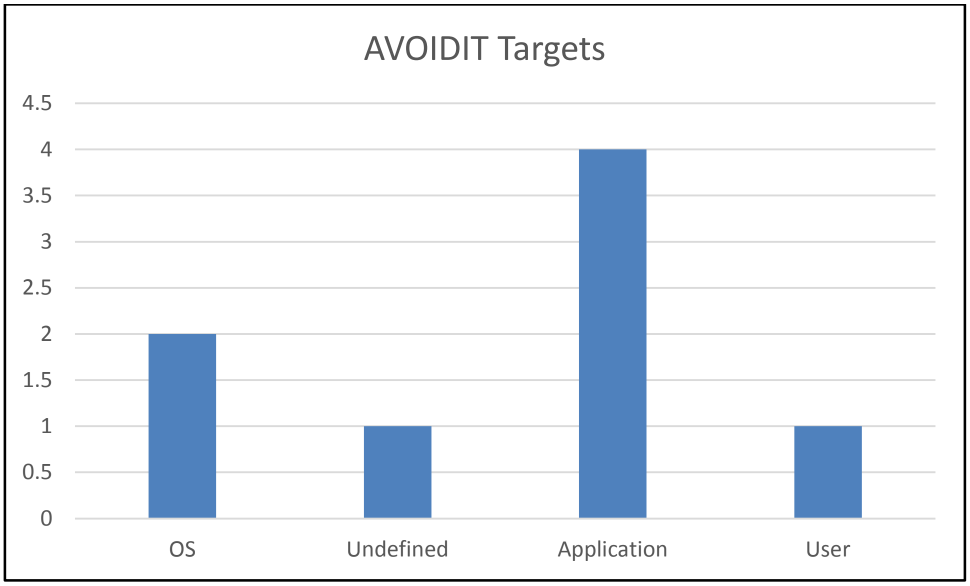




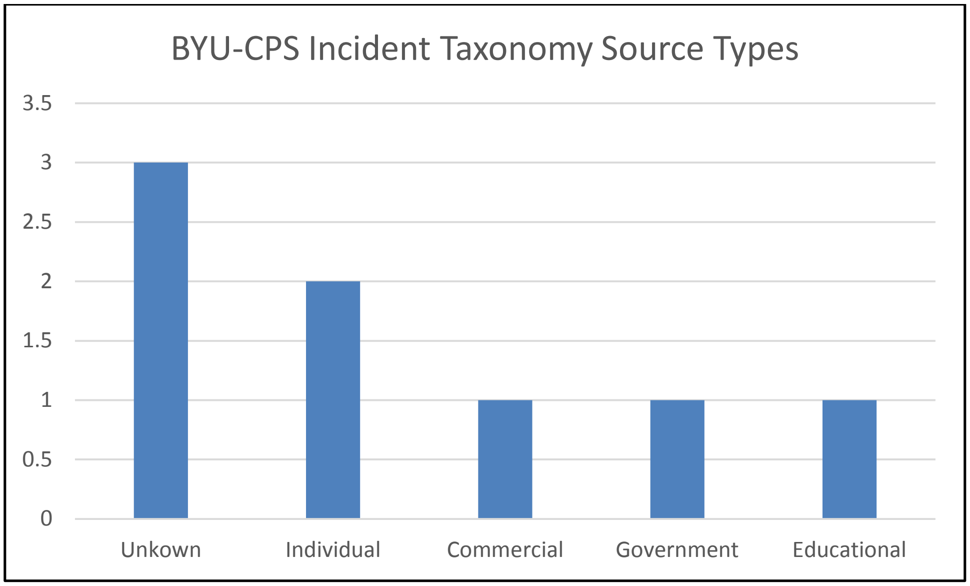

AVOIDIT Mitigations
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Remove from Network
Undefined
Unknown
None

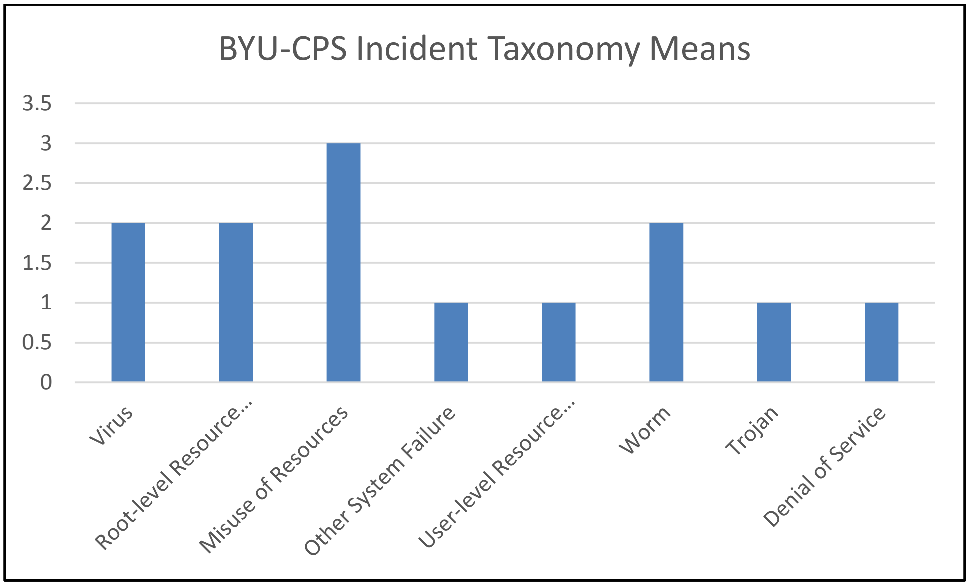

AVOIDIT Remediations
3.5
3
2.5
2
1.5
1
0.5
0
Correct Code
Patch System
Undefined
Unknown
None

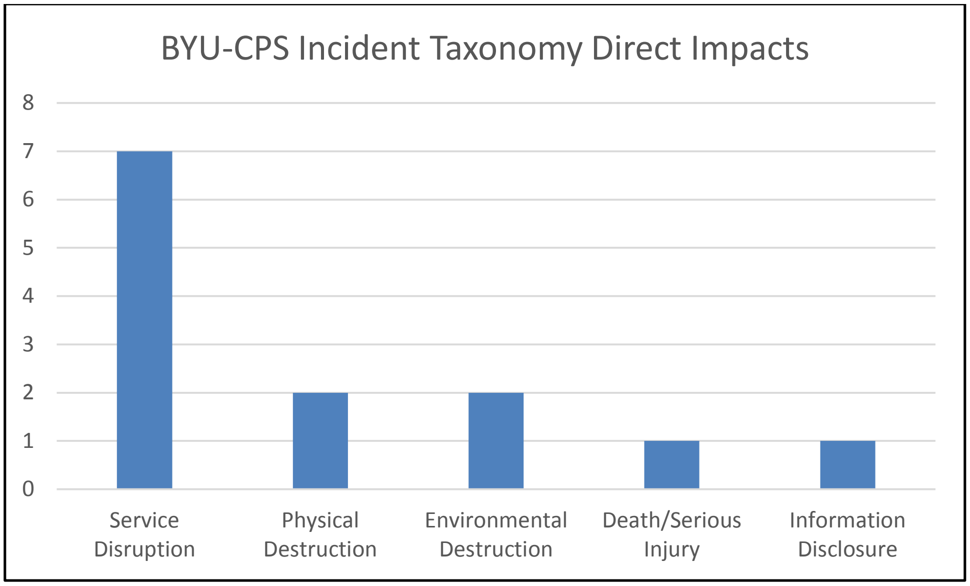

AVOIDIT Informational Impacts
7
6
5
4
3
2
1
0
Disrupt
Undefined
Distort
Disclosure

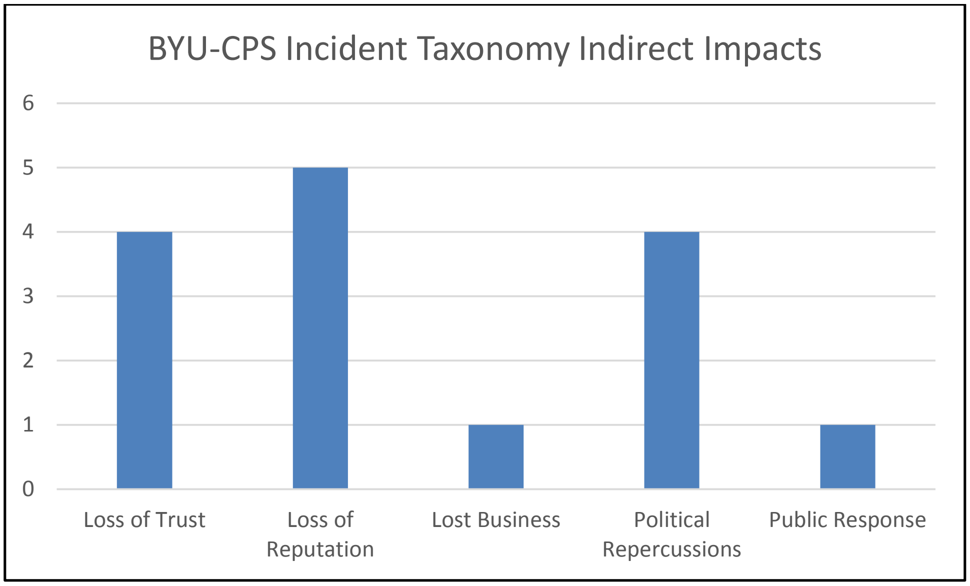

AVOIDIT Targets
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
OS
Undefined
Application
User

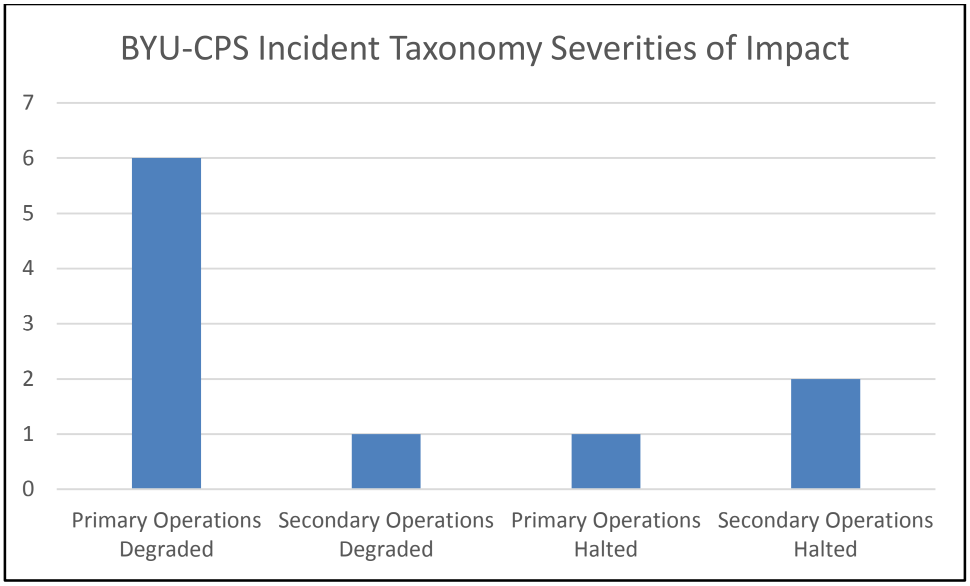
The following figures present the distribution of classifications according to the new taxonomy.

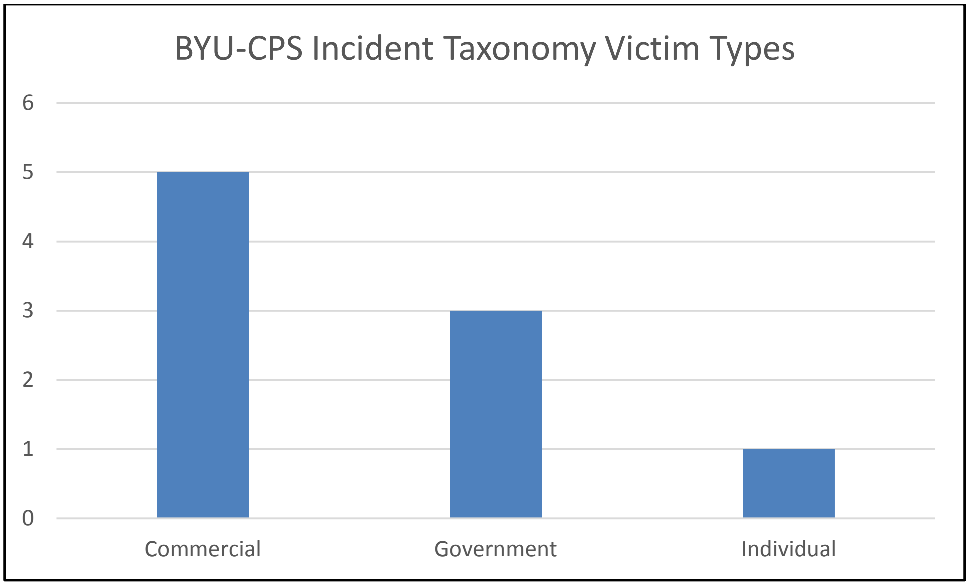


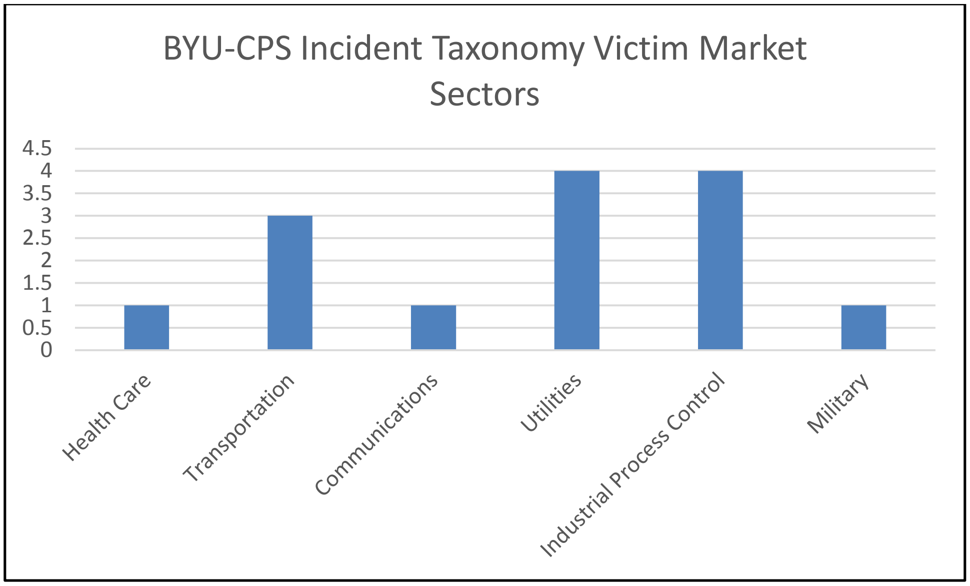



BYU-CPS Incident Taxonomy Direct Impacts
8
7
6
5
4
3
2
1
0
Service Disruption
Physical Destruction
Environmental Destruction
Death/Serious Injury
Information Disclosure


BYU-CPS Incident Taxonomy Indirect Impacts
6
5
4
3
2
1
0
Loss of Trust
Loss of Reputation
Lost Business
Political Repercussions
Public Response


BYU-CPS Incident Taxonomy Severities of Impact
7
6
5
4
3
2
1
0
Primary Operations Degraded
Secondary Operations Degraded
Primary Operations Halted
Secondary Operations Halted


BYU-CPS Incident Taxonomy Victim Types
6
5
4
3
2
1
0
Commercial
Government
Individual


BYU-CPS Incident Taxonomy Victim Market Sectors
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Health Care
Transportation
Communications
Utilities
Industrial Process Control
Military